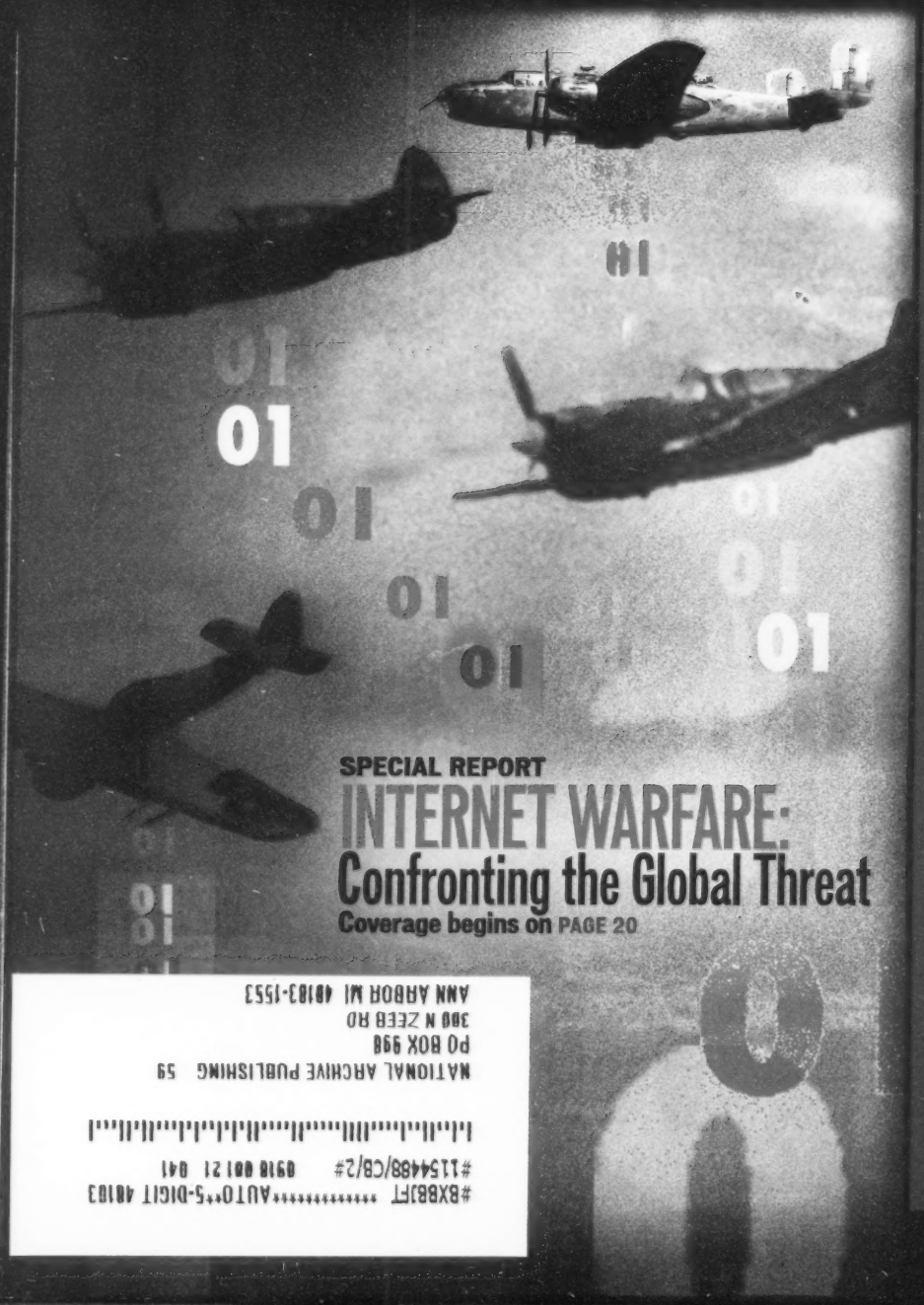
The Grill: Entrepreneur Gregg Favalora talks about IT breakthroughs in 3-D medical imaging that help surgeons zero in on 'where to snip.' PAGE 15

COMPUTERWORLD®



SPECIAL REPORT

INTERNET WARFARE: Confronting the Global Threat

Coverage begins on PAGE 20

#8X8BJFT ********AUTO**5-DIGIT 48103
#11544B8/CB/2# 0910 001 21 041
NATIONAL ARCHIVE PUBLISHING 59
PO BOX 990
300 N ZEEB RD
ANN ARBOR MI 48103-1553

Inside

APRIL 27, 2009
VOL. 43, NO. 16 $5/COPY

News & Analysis

Should the White House be leading national cybersecurity efforts? PAGE 6

Oracle's plan to buy Sun raised a lot more questions than the vendor was willing to answer. PAGE 10

VMware claims it has built an OS for virtual clouds. That may not be *all* hype. PAGE 14

Opinion

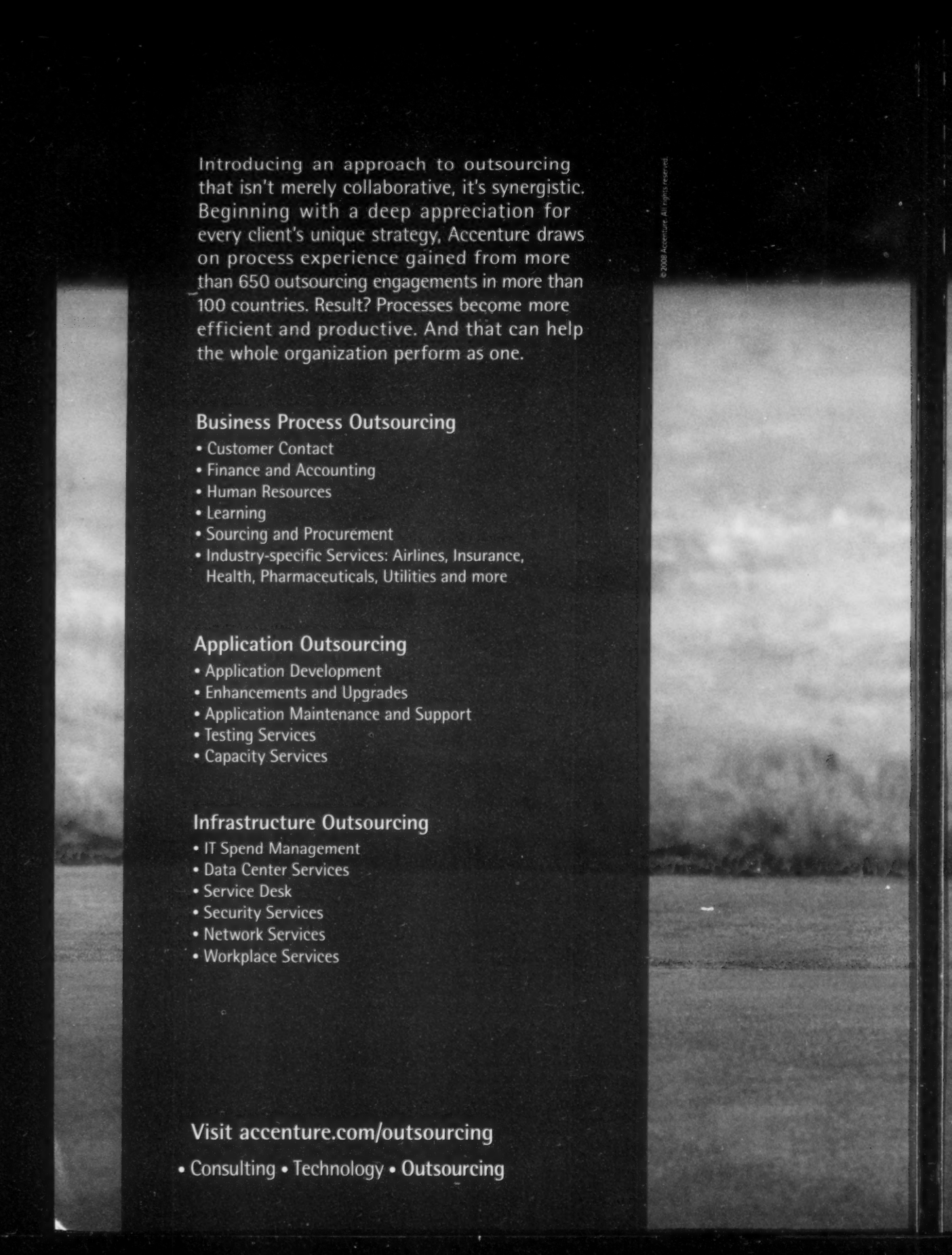
Steven J. Vaughan-Nichols says that Microsoft is doing something right. Well, half right. PAGE 18

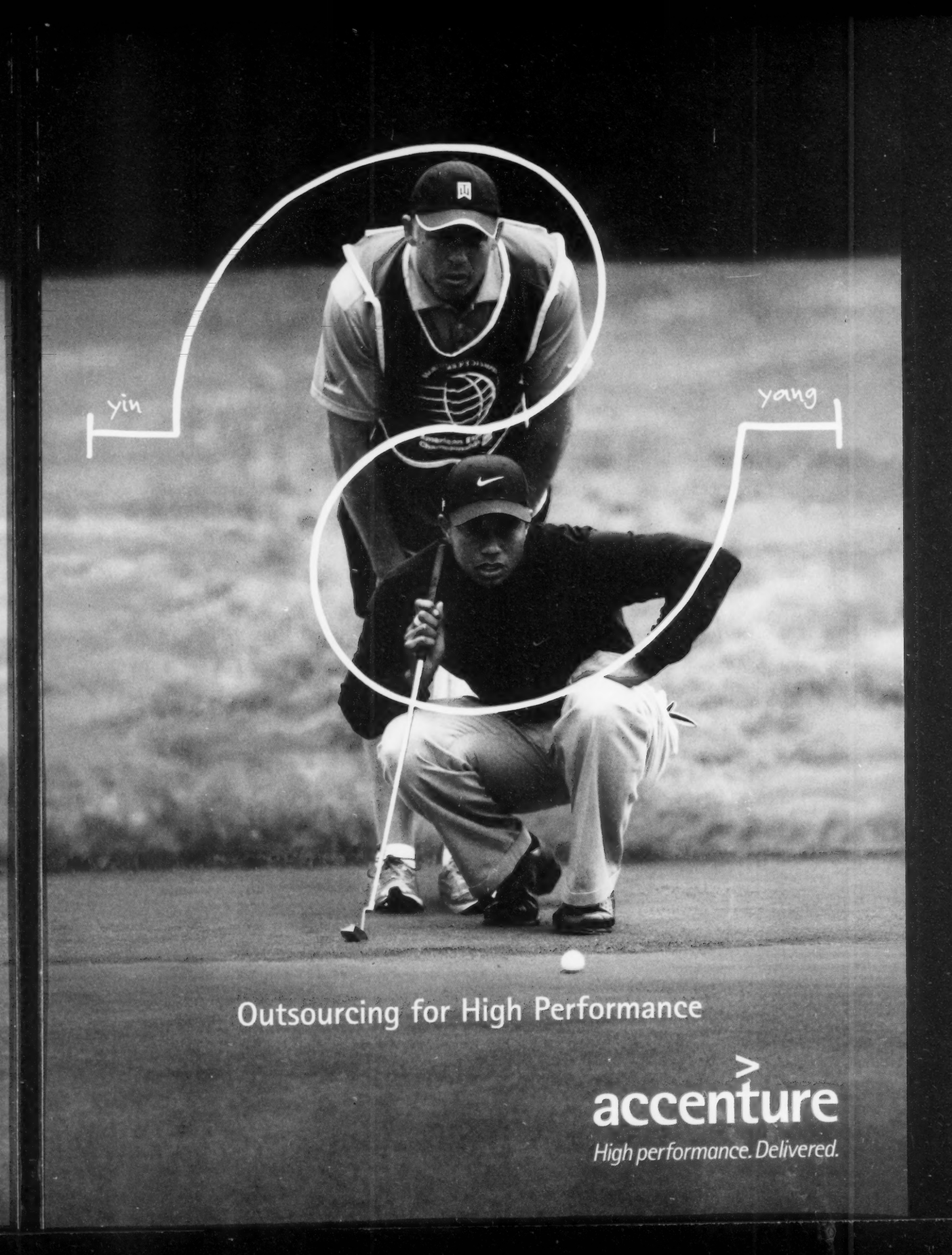
Security

A play-by-play on how one IT shop prepared for Conficker. PAGE 33

Careers

When should you bring up the topic of money in a job interview? PAGE 36


Introducing an approach to outsourcing that isn't merely collaborative, it's synergistic. Beginning with a deep appreciation for every client's unique strategy, Accenture draws on process experience gained from more than 650 outsourcing engagements in more than 100 countries. Result? Processes become more efficient and productive. And that can help the whole organization perform as one.
Business Process Outsourcing
• Customer Contact
• Finance and Accounting
• Human Resources
• Learning
• Sourcing and Procurement
• Industry-specific Services: Airlines, Insurance, Health, Pharmaceuticals, Utilities and more
Application Outsourcing
• Application Development
• Enhancements and Upgrades
• Application Maintenance and Support
• Testing Services
• Capacity Services
Infrastructure Outsourcing
• IT Spend Management
• Data Center Services
• Service Desk
• Security Services
• Network Services
• Workplace Services
Visit accenture.com/outsourcing
• Consulting • Technology • Outsourcing
© 2008 Accenture. All rights reserved.


yin
yang
Outsourcing for High Performance
accenture
High performance. Delivered.

■ NEWS

6 The official who oversaw a federal **cybersecurity review** says the **White House** should **lead** public- and private-sector initiatives. | **Microsoft** says users will see **UAC pop-up messages** a lot less often in **Windows 7** than they do in Vista.

7 A study finds that using **H-1B workers** reduces **IT salaries** by as much as 6%. | **AMD** plans to release a six-core **Opteron chip** in June and offer **16 cores** by 2011.

8 The **Pentagon,** which signed a **$40 million** systems order with **SGI** in January, is watching closely as the **HPC vendor** sells its assets.

10 **Oracle Leaves 'Em Wanting More on Its Plans for Sun.** The announcement that Oracle is buying Sun Microsystems raises a lot more questions about the future of Sun's technologies than Oracle officials were willing to answer last week.

14 **VMware Looks to Bring Data Centers Under the Cloud.** VMware hopes its new vSphere software will persuade IT managers to virtualize their data centers. But some key features are missing.

■ OPINION

4 **Don Tennant** says the private sector must be a full-fledged combatant in any cyberwar.

18 **Steven J. Vaughan-Nichols** finds that Microsoft is actually doing something right – well, half right.

34 **Preston Gralla** believes that privacy will be the first casualty in the era of cyberwarfare.

40 **Frank Hayes** says the Oracle-Sun deal will give Larry Ellison another chance to have a hit with appliances.

■ DEPARTMENTS

15 Imaging pioneer **Gregg Favalora** talks about "crystal ball" 3-D imaging, breakthrough medical applications and entrepreneurial best practices.

33 **Attention to Conficker Seems to Pay Off.** The notorious worm has Mathias Thurman's security team putting all of its focus on protecting the company's 9,000 systems around the globe.

36 *Computerworld* Premier 100 IT Leader Mark Burnette discusses how to keep your head while your co-workers are losing theirs to the job-cutting ax. Plus, at what point in the job application process should you bring up the touchy subject of salary?

38 "I am a phone on a smart switch. Temperature rising. Must shut down. Then must send out alert about rising temperature."

■ ALSO IN THIS ISSUE

Online Chatter 5

Company Index 38

20

■ SPECIAL REPORT

INTERNET WARFARE: Confronting the Global Threat

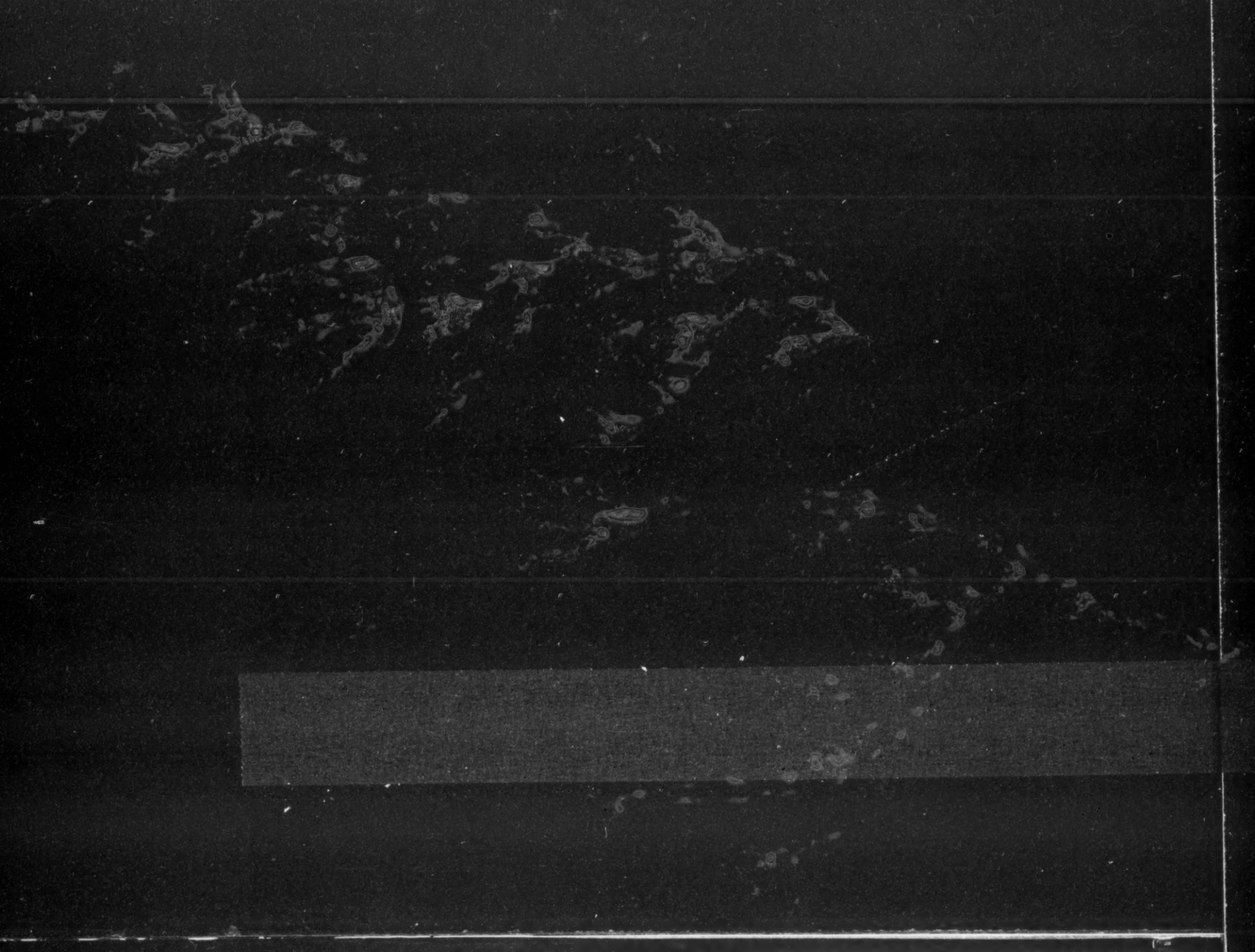
20 Are We Focused on The Wrong Things?

More than seven years after 9/11, federal efforts to secure the country's cyberinfrastructure are bogged down by a lack of vision, planning and leadership. Here are six steps the new administration should take now.

28 The Fog of (Cyber) War

Cybermilitias, black hat hackers and other non-nation-state bad guys obscure the battlefield. How do you stop an enemy you can't identify?

28



Inside

COMPUTERWORLD ■ APRIL 27, 2009

■ NEWS

6 The official who oversaw a federal **cybersecurity review** says the **White House** should **lead** public- and private-sector initiatives. | **Microsoft** says users will see **UAC pop-up messages** a lot less often in **Windows 7** than they do in Vista.

7 A study finds that using **H-1B workers** reduces **IT salaries** by as much as 6%. | **AMD** plans to release a six-core **Opteron chip** in June and offer **16 cores** by 2011.

8 The **Pentagon,** which signed a **$40 million** systems order with **SGI** in January, is watching closely as the **HPC vendor** sells its assets.

10 Oracle Leaves 'Em Wanting More on Its Plans for Sun. The announcement that Oracle is buying Sun Microsystems raises a lot more questions about the future of Sun's technologies than Oracle officials were willing to answer last week.

14 VMware Looks to Bring Data Centers Under the Cloud. VMware hopes its new vSphere software will persuade IT managers to virtualize their data centers. But some key features are missing.

■ OPINION

4 Editor's Note: **Don Tennant** says the private sector must be a full-fledged combatant in any cyberwar.

18 Steven J. Vaughan-Nichols finds that Microsoft is actually doing something right – well, half right.

34 Preston Gralla believes that privacy will be the first casualty in the era of cyberwarfare.

40 Frankly Speaking: **Frank Hayes** says the Oracle-Sun deal will give Larry Ellison another chance to have a hit with appliances.

■ DEPARTMENTS

15 The Grill: Imaging pioneer **Gregg Favalora** talks about "crystal ball" 3-D imaging, breakthrough medical applications and entrepreneurial best practices.

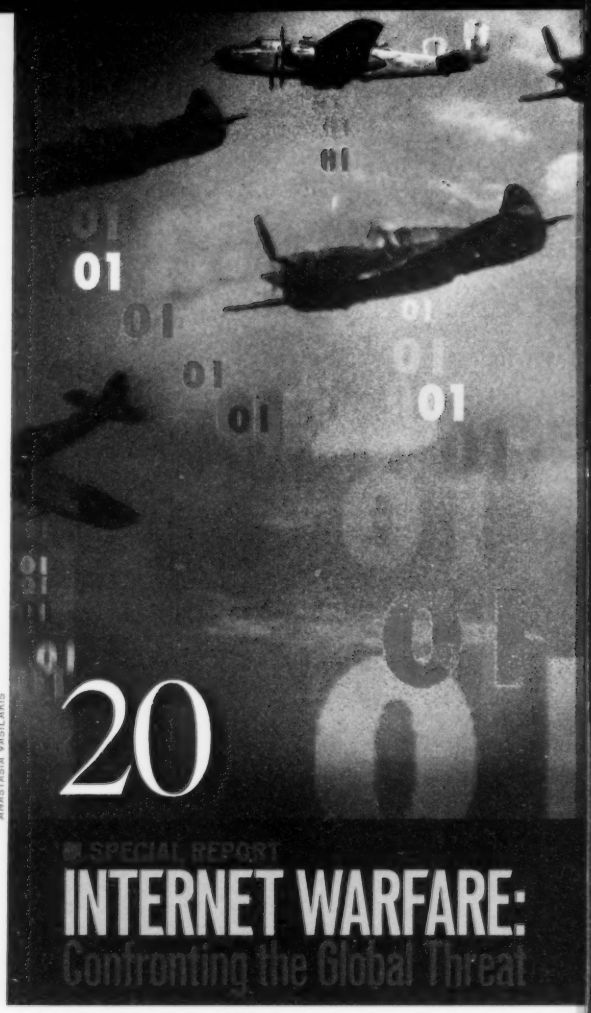
33 Security Manager's Journal: **Attention to Conficker Seems to Pay Off.** The notorious worm has Mathias Thurman's security team putting all of its focus on protecting the company's 9,000 systems around the globe.

36 Career Watch: *Computerworld* Premier 100 IT Leader Mark Burnette discusses how to keep your head while your co-workers are losing theirs to the job-cutting ax. Plus, at what point in the job application process should you bring up the touchy subject of salary?

38 Shark Tank: "I am a phone on a smart switch. Temperature rising. Must shut down. Then must send out alert about rising temperature."

■ ALSO IN THIS ISSUE

Online Chatter	5
Company Index	38



ANASTASIA VASILARIS

■ SPECIAL REPORT

INTERNET WARFARE: Confronting the Global Threat

20 Are We Focused on The Wrong Things?

More than seven years after 9/11, federal efforts to secure the country's cyberinfrastructure are bogged down by a lack of vision, planning and leadership. Here are six steps the new administration should take now.

28 The Fog of (Cyber) War

Cybermilitias, black hat hackers and other non-nation-state bad guys obscure the battlefield. How do you stop an enemy you can't identify?

© FOTOLIA / FLASHPIX

VIRTUALIZATION FOR WINDOWS SERVER 2008 AND SUSE LINUX ENTERPRISE SIMPLIFIES THE DATA CENTER.

AND THE CALL CENTER.

INTEROP ABILITY RUN WITH IT.

It's the virtualization solution that comes with joint support from Microsoft® and Novell® that figures out the hard stuff for you. With it, you can bring Windows Server® 2008 and SUSE® Linux Enterprise Server together securely and reliably, with clearly defined intellectual property rights. So you can build your data center the way you want to and go virtual — without headaches or hassles.

Need the best Linux? Request your SUSE Linux Enterprise deployment kit and workshop now at moreinterop.com

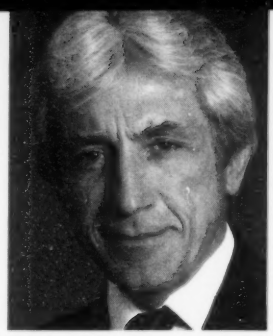
Novell® Microsoft®

Copyright © 2008 Novell, Inc. and Microsoft Corporation. All Rights Reserved. Novell, the Novell logo and SUSE are registered trademarks of Novell, Inc. in the United States and other countries. *Linux is a registered trademark of Linus Torvalds. Microsoft and Windows Server are trademarks of the Microsoft group of companies.

■ EDITOR'S NOTE

Don Tennant

Whatever It Takes



IN THE FILM *State of Play*, a thriller now playing in a theater near you, the bad guys are tied to a Blackwater-like security contractor called Point Corp. The contractor is out to make a killing, so to speak, by persuading congressional leaders to outsource homeland security to the private sector. Billions of dollars in potential contracts are at stake, so the bad guys are determined to do whatever it takes.

Back in the real world, the U.S. House Committee on Homeland Security doesn't have to deal with Point Corp., but it certainly has its hands full. As Jaikumar Vijayan reports in this week's special report on Internet warfare (page 20), the committee held a hearing last month on U.S. readiness to counter the cyberwarfare threat. Five witnesses representing the government and the private sector testified. Asked whether they felt the federal government is prepared to deal with a cybercatastrophe, each said no.

If that prompts you to point a finger at the government, don't be too quick to condemn bureaucratic incompetence. The question of whether the government is prepared for a cybercatastrophe is the wrong one to ask. It's not a matter of whether the federal government is prepared. It's a matter of whether *we* as a nation are prepared. We can't dump this one on the government.

That's not to say that the answer lies in outsourcing cyberdefense to the likes of a private-sector firm such as Point Corp. What we need to understand is that whereas national defense is fundamentally the domain of government in traditional warfare, in cyberwarfare it is at least as much the domain of the private sector. The reason: We're all standing squarely in the line of fire. The private sector is no longer simply a supplier to or supporter of our national defense efforts. It's now a full-fledged combatant in the war.

When the news broke last week that hackers had breached the Pentagon's F-35 Joint Strike Fighter project, the security of Defense Department systems was only part of the story. According to *The Wall Street Journal*, which cited sources who had been briefed on the matter, the hackers succeeded in breaching the systems by penetrating the networks of two or three contractors. Lockheed Martin is the lead contractor on the project, with Northrop Grumman and BAE Systems playing major roles, the *Journal* reported.

■ The private sector is no longer simply a supplier and supporter. It's now a full-fledged combatant in the war.

More to the point, private-sector combatants aren't limited to companies in the defense industry but are found in multiple industries that constitute our nation's critical infrastructure. Reports earlier this month that the power grid had been penetrated by hackers, possibly from China and/or Russia, raised plenty of eyebrows but seemed largely forgotten by the next news cycle.

Given that our critical infrastructure, from energy and utilities to health care and financial services, is owned and operated almost entirely by the private sector, it's nonsensical to think that we can leave it to the federal government to fight our cyberwar. I recently discussed this topic with Paul Kurtz, former senior director for critical infrastructure protection on the White House's Homeland Security Council, who said the government is properly and necessarily focused on securing its own data first.

"To me, what that underscores is that the private sector can't wait for government," Kurtz said. He cited the energy sector as especially lax, but he stressed that he's concerned about "high-tech areas — pharmaceuticals, biogenetics, IT, alternative energy, aviation — that are going to fuel our economic growth over the long haul. That's our future," Kurtz said. "And we're losing it every day because they're not adequately securing their systems."

The government's task is to mobilize the private sector — by means of tax incentives, loans or whatever fiscal devices make sense — to fight the cyberwar. Then the private sector needs to do whatever it takes to fight it and win. That's what combatants do. ■

Don Tennant *is Computerworld's senior editor-at-large. You can contact him at don_tennant@computerworld.com, visit his blog at* http://blogs.computerworld.com/tennant, *and follow him on Twitter at* http://twitter.com/dontennant.

RESPONSES TO:

'Mafiaboy' Spills the Beans at IT360 on Underground Hackers

April 14, 2009

A jewel of Michael Calce's insider "knowledge": "Calce said his own systems have never been compromised. 'I run Unix servers, so I'm constantly maintaining. I'm always watching the logs. Unless there is someone in my systems who is very undetectable, to my knowledge, nothing has been tampered with.' "

Brilliant! No real security pro would make such a moronic statement. This stuff is what you would learn from "Hacking For Dummies."
■ **Submitted by:** *Matt*

I would not hire a so-called ex-hacker. The first reason is the obvious: no respect for the law. The second one is a bit more subtle. Really good black-hat hackers are people you'll never hear about. And they don't tell people their secrets, any more than a fisherman would advertise his hot fishin' spot.
■ **Submitted by:** *Fjardeson*

I don't have a problem with hiring an ex-hacker as long as he is closely supervised initially and given limited tasks. However, I believe this approach should be taken with all new hires. Too often, we hire a SA and give him/her the keys to the kingdom the first day.
■ **Submitted by:** *Striker*

As an ex-cracker who now works as a security adviser, I can honestly say I would never betray the trust of a client or steal/damage their systems in any way. After all, I'm trying to run a legitimate business and make a living for myself. Even though I did some black-hat hacking as a teenager, I've grown to see the difference of right and wrong and have learned to respect the legal boundary. People can change. A lot of us do stupid things as teenagers. No doubt most of us would have defaced a Web site as a prank or fooled around with netbus/subseven if we had known how to.
■ **Submitted by:** *Anonymous*

JOIN THE CHATTER! *You, too, can comment directly on our stories, at* **computerworld.com.**

COMPUTERWORLD.COM

Find these stories at computerworld.com/more

Living on Air

Windows expert Preston Gralla was challenged to work with Mac OS X for two weeks. Will he ever go back to a PC after using Apple's Air?

Customers and Clients And Consumers, Oh My!

Why the labels you use to identify your users matter.

Recycle Your Tech Gear – It's Easier Than You Think

There are a lot of places online that can make it easier to sell, recycle or give away those old monitors, computers, phones and cameras.

Free Sites That Can Help You Manage Your Money

REVIEW: We take a look at Web sites that aim to help you manage your finances, set a budget and get out of debt.

Who Wins, Who Loses In an Oracle-Sun Deal?

Oracle wins, certainly, and – to a certain extent – Sun does too. Users? Not so much.

COMPUTERWORLD

P.O. Box 9171, 1 Speen Street
Framingham, MA 01701
(508) 879-0700
Computerworld.com

■ **EDITORIAL**

Editor in Chief Scot Finnie

Senior Editor-at-Large Don Tennant

Executive Editors Mitch Betts, Julia King (events)

Managing Editors Michele Lee DeFilippo (production), Sharon Machlis (online), Ken Mingis (news)

Design Director Stephanie Faucher

Director of Blogs Joyce Carpenter

Technologies Editor Johanna Ambrosio

Features Editors Kathleen Melymuka, Valerie Potter, Ellen Fanning (special reports), Barbara Krasnoff (reviews)

Senior Editor Mike Barton (new media)

Senior News Editor Craig Stedman

News Editors Mike Bucken, Marian Prokop

National Correspondents Gary Anthes, Julia King, Robert L. Mitchell

Reporters Sharon Gaudin, Matt Hamblen, Gregg Keizer, Eric Lai, Lucas Mearian, Patrick Thibodeau, Jaikumar Vijayan

Features Writer, Video Editor David Ramel

Assistant Managing Editor Bob Rawson (production)

Senior News Columnist Frank Hayes

Art Director April Montgomery

Research Manager Mari Keefe

Senior Copy Editors Eugene Demaitre, Monica Sambataro

Copy Editor Donna Sussman

Associate Editor, Community Ken Gagné

Office Manager Linda Gorgone

Contributing Editors Jamie Eckle, Preston Gralla, Tracy Mayor

■ **CONTACTS**

Phone numbers, e-mail addresses and reporters' beats are available online at *Computerworld.com* (see Contacts link at the bottom of the home page).

Letters to the Editor Send to letters@computerworld.com. Include an address and phone number for immediate verification. Letters will be edited for brevity and clarity.

News tips newstips@computerworld.com

Subscriptions and back issues (888) 559-7327, cw@omeda.com

Reprints/permissions The YGS Group, (800) 290-5460, ext. 148, computerworld@theygsgroup.com

News Digest

FIND THE FULL STORIES AT COMPUTERWORLD.COM

THE WEEK AHEAD

MONDAY: The Computer Forensics Show, which focuses on recovering data from systems, opens in Washington.

TUESDAY: Sun, which agreed to be bought by Oracle last week (see story, page 10), is due to report its third-quarter results.

TUESDAY: The Microsoft Management Summit 2009 begins in Las Vegas, focusing on the vendor's IT management tools.

WEDNESDAY: SAP plans to file its Q1 earnings report.

Melissa Hathaway, the federal government's acting senior director for cyberspace, says agencies don't have a broad view of security threats.

IT AND GOVERNMENT

Cybersecurity Official Says White House Should Lead

THE FEDERAL official who led a 60-day review of the U.S. government's cybersecurity programs for President Barack Obama last week called for the White House to play a more direct role in coordinating national information security efforts.

Speaking at the RSA Conference 2009 in San Francisco, Melissa Hathaway, who completed her review on April 17, said that collaboration between the private and public sectors is needed to protect critical systems. But, she added, the task of leading cybersecurity efforts "is the fundamental responsibility of our government."

And in arguing for a larger White House role, Hathaway claimed that the government's leadership mandate transcends the purviews of individual agencies, none of which has "a broad enough perspective to match the sweep of the challenges." Based on her review, it's clear that the government isn't "organized appropriately" to address cyberthreats, Hathaway said. Many of the agencies that are involved have overlapping authority, she noted.

Hathaway's comments added to the growing chorus of voices calling for a substantial overhaul of federal cybersecurity processes.

Earlier this month, Sens. Olympia Snowe (R-Maine) and Jay Rockefeller (D-W.Va.) introduced legislation to give federal officials new powers to set security standards and policies for agencies and key industries. A companion bill would create a cybersecurity office within the White House.

The bills are largely based on recommendations made by a commission set up by the Center for Strategic and International Studies. Tom Kellerman, a vice president at Core Security Technologies and a commission member, said last week that White House leadership is "paramount" to the success of cybersecurity efforts.

In another RSA speech, Lt. Gen. Keith Alexander, director of the National Security Agency, said the NSA isn't looking to take control of the national cybersecurity agenda, as some have claimed. Instead, the spy agency wants to work with the Department of Homeland Security to provide the "technical support" needed to combat cyberthreats, he said.

— Jaikumar Vijayan

OPERATING SYSTEMS

Microsoft Cuts UAC Prompts In Windows 7

User Account Control, a Windows Vista security feature that has long been considered intrusive, will appear about one-third less often in Windows 7 than it does in Vista.

"From our beta and internal testing, we expect a 29% decrease in UAC prompts compared to Windows Vista," Paul Cooke, Microsoft Corp.'s director of Windows 7 client enterprise security, said last week.

The UAC feature is designed to reduce the chance that malware could hijack a PC by forcing users to confirm that they really intend to do things such as install software or modify key settings.

Earlier this year, Jon DeVaan, senior vice president of Microsoft's Windows core operating system unit, said the move to scale back UAC prompts came after an internal study found that users were suffering from "click fatigue."

– GREGG KEIZER

Microsoft had already modified the Windows 7 User Account Control after critics argued it could easily be disabled by attackers.

CAREERS

Study Finds H-1B Use Cuts Tech Wages by Up to 6%

THE USE of H-1B workers by U.S. companies is decreasing wages by as much as 6% for some IT workers, according to a study by researchers at New York University's and the University of Pennsylvania's business schools.

The study, released earlier this month by professors from the Stern and Wharton schools of business, concluded that H-1B workers' entry into the U.S. at current levels is causing a 5% to 6% drop in wages for computer programmers, systems analysts and software engineers. The study also found that offshore outsourcing decreases wages for a broader category of workers, including IT managers, by 2% to 3%.

The IT workers most likely to be affected by the downward pressure on wages are recent college graduates and people changing jobs, the researchers said.

The authors of the study, Prasanna Tambe, an assistant professor at Stern, and Lorin Hitt, a professor at Wharton, said they used data from multiple sources, including a "leading online job search site" that they wouldn't identify. Tambe and Hitt said they combined the demographic and wage data of individual companies available at the job-search site with information on H-1B visas and outsourcing available through the government and other public sources.

The study was based on information compiled on 156,000 IT workers employed at nearly 7,500 publicly held U.S. firms, Tambe and Hitt said. The data from the combined sources provided what they called a "micro-data" view of public companies that hire H-1B visa holders and offshore workers.

The goal of the study was to "precisely look at how domestic workers are being affected by globalization," Tambe said. "I'm not making a judgment on whether that is good or bad."

In addition, the researchers wrote, "we simply sought to dispel the myth that globalization generates no losers" and to provide U.S. policymakers with data on how the H-1B program affects IT wages.

They did urge lawmakers to carefully weigh the effects of globalization on workers "against the macro-level economic effects."

"Offshoring will most likely remain a necessary and important part of the global economy," the authors said. "There is substantial evidence that H-1B admissions appear to directly improve levels of innovation and entrepreneurship, which in the long term should create new jobs and raise demand for technology workers in other areas."

— *Patrick Thibodeau*

Short Takes

- EMC Corp. announced a 5% pay cut for all salaried employees after reporting that its first-quarter profits plummeted 23%, from $251.6 million a year ago to $194.1 million. Sales in the quarter fell 9.2% to $3.15 billion.
- Citing the poor economy and falling PC sales, Microsoft Corp. reported that its first-quarter revenue declined 6% from a year earlier, to $13.65 billion. Sales in the company's Windows client unit dropped to $3.4 billion from $4 billion last year.
- NASA's Ames Research Center announced last week that it has swapped out 10 tape silos from Sun Microsystems Inc. for two Spectra Logic Corp. T950 products, consolidating its tape libraries and increasing capacity from 12 to 32 petabytes.
- Broadcom Corp. has made a hostile $764 million bid to purchase Emulex Corp. The offer comes three months after Emulex rejected overtures from the semiconductor maker.

PROCESSORS

AMD to Ship Six-Core Chip in June, Plans 16 Cores by 2011

Advanced Micro Devices Inc. last week said it will release a six-core Opteron processor in June, five months ahead of schedule. And it detailed plans to add chips supporting up to 12 cores next year and 16 in 2011.

AMD, which reported a $416 million first-quarter loss last week, said the six-core server chip, code-named Istanbul, will provide up to a 30% performance boost over current quad-core Opterons while using the same amount of power.

Istanbul will be followed early next year by a chip code-named Magny-Cours, which will ship in eight- and 12-core models, AMD said. And in 2011, the company plans to release a processor called Interlagos, which will be offered with 12 and 16 cores.

Opteron Road Map

JUNE: Istanbul six-core processor, AMD's first with more than four cores

2010: Magny-Cours chip with eight and 12 cores, plus the lower-end Lisbon processor with four and six cores

2011: Interlagos with 12 and 16 cores, and Valencia with six and eight, both built using a 32-nanometer process

Insight64 analyst Nathan Brookwood said AMD is trying to get ahead of Intel Corp., which released its six-core Xeon 7400 server chip last September and plans to add an eight-core processor code-named Nehalem EX next year.

Intel "clearly has seized the performance advantage" in the server market, he said, but AMD officials think Istanbul "will keep them very competitive over the next year, and then going to 12 cores in 2010 will keep them competitive when Intel comes out with eight."

– PATRICK THIBODEAU

HARDWARE

SGI Sale Puts Pentagon on Guard Over $40M Order

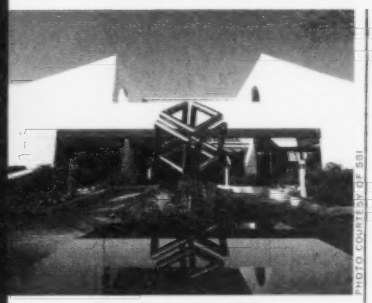


PHOTO COURTESY OF SGI

<< The Sunnyvale, Calif., home of SGI, which won a Pentagon contract despite its financial problems.

IN JANUARY, Silicon Graphics Inc. was in a downward spiral that eventually led to an April 1 deal to sell its assets to Rackable Systems Inc. for just $25 million. But that didn't stop the U.S. Department of Defense from signing a $40 million systems contract with SGI.

Cray Henry, head of the DOD's High-Performance Computing Modernization Program, said this month that SGI's "financial situation was not as strong as we would have liked" in January. But, he added, the Pentagon went ahead with the multiyear contract that month for six systems because it believed that the company was still "financially responsive."

Now the DOD is watching the situation closely. Henry said he expects "significant uncertainty" until the end of May, which is when Rackable expects to complete the asset purchase. But both companies "tell us they are committed to maintaining the systems we purchased in prior years and delivering the systems we ordered for delivery this year," he said.

The first of the Xeon-based Altix systems that the Pentagon ordered from SGI is scheduled to be delivered this month. The machines will be installed at five research-and-development facilities in the U.S., said SGI.

Henry isn't the only SGI user who's keeping an eye on the high-performance computing vendor. Gabe Turner, a systems administrator in the HPC group at the Minnesota Supercomputing Institute in Minneapolis, said that his biggest concern is the future of SGI's customer support.

"We've got support contracts that are just over a year old, and what is the state of SGI going to be two years from now?" Henry said. "I just have no idea."

— Patrick Thibodeau

BETWEEN THE LINES *By John Klossner*

BENCHMARKS LAST WEEK

President Barack Obama named Aneesh Chopra the federal government's first chief technology officer. Chopra, who had been Virginia's secretary of technology, will work with Vivek Kundra, the first federal CIO.

VMware Inc. said its quarterly revenue may drop year-to-year for the first time ever because of the economy and a product transition.

THREE YEARS AGO: Sun Microsystems Inc. cofounder Scott McNealy stepped down as CEO. He was replaced by Sun's president, Jonathan Schwartz, but stayed on as chairman.

Global Dispatches

Sony Ericsson Cuts 2,000 More Jobs

LONDON – Struggling Sony Ericsson Mobile Communications AB earlier this month announced plans to cut another 2,000 jobs after reporting that its shipments and market share dipped during the first quarter. The company had already carried out a layoff of 2,000 workers that was announced late last year.

The cell phone manufacturer, based here, had reported on April 16 that its first-quarter sales fell 27% to €1.74 billion ($2.28 billion U.S.) from €2.7 billion a year earlier, and that unit shipments dropped 35% during the same period. Sony Ericsson attributed the poor performance to weak consumer confidence and a decline in new orders from retailers.

Nancy Gohring,
IDG News Service

Tata's Profit Drops 10.1% to $1.12B

MUMBAI, India – Tata Consultancy Services Ltd. last week reported that its fiscal 2009 profit fell by 10.1% to $1.12 billion, on revenue that rose 6% to $6 billion.

Tata's chief operating officer, N. Chandrasekaran, said Indian outsourcers are facing a slowdown in business because clients are postponing discretionary projects and trying to renegotiate existing contracts.

The company's chief financial officer, Seturaman Mahalingam, said Tata expects prices for its services to decline by less than 10% this year.

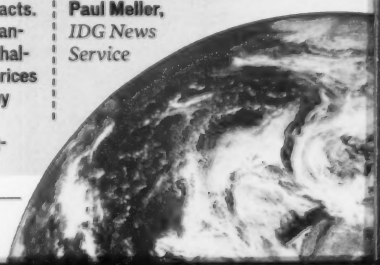
Tata, India's largest outsourcer, employed 143,761 people at the close of its fiscal year on March 31, up 32,354 from a year earlier.

John Ribeiro,
IDG News Service

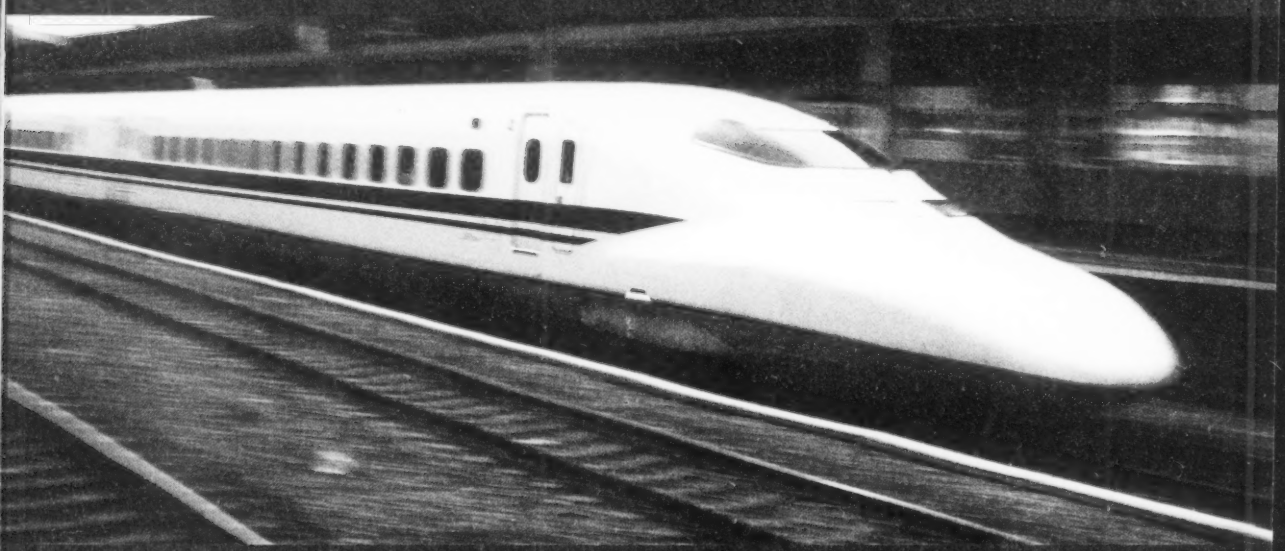
BRIEFLY NOTED

Two trade groups – the Pan-European ICT and eBusiness Network for SMEs, and the Association for Competitive Technology – have joined as interested parties in the European Commission's antitrust case against Microsoft Corp. The EC contends that Microsoft's bundling of the Internet Explorer browser with the Windows operating system hampers competition.

Paul Meller,
IDG News Service



KEEP ONLINE TRANSACTIONS FAST AND TIME-TO-VALUE FASTER.



CA Wily Application Performance Management is designed to improve the performance and availability of mission critical and revenue-generating applications. So you can quickly spot and correct online production application incidents before they become customer problems — especially in complex and high volume transaction environments. That's the power of lean.

Learn more at ca.com/apm

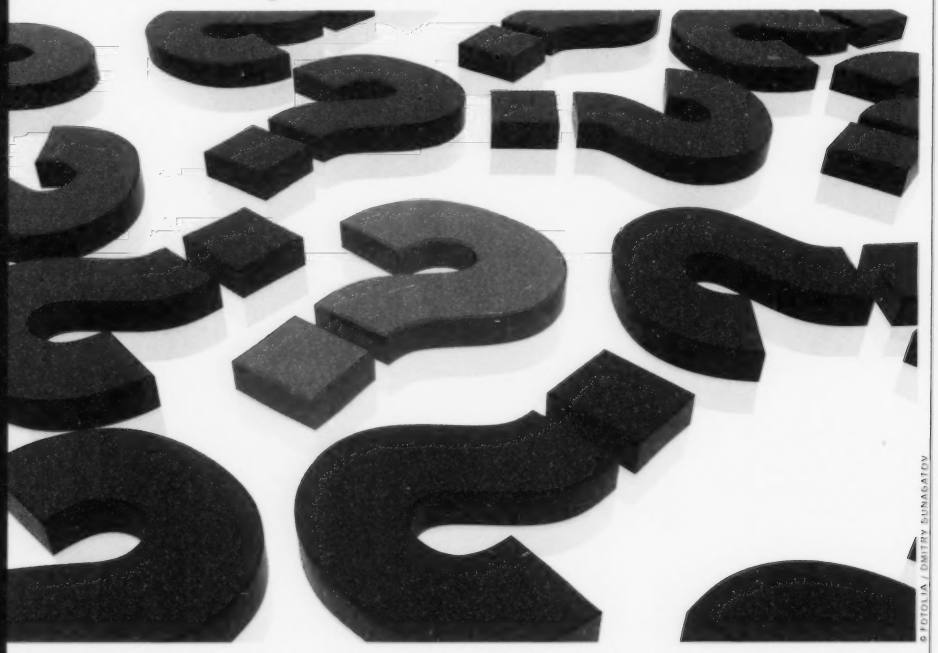
ca Software

Copyright © 2009 CA. All rights reserved.

■ NEWS ANALYSIS

Oracle Leaves 'Em Wanting More on Its Plans for Sun

The software vendor hasn't said much about what it intends to do after buying Sun. Users are waiting for answers. **By Patrick Thibodeau**



© FOTOLIA / DMITRIY SUNAGATOV

ORACLE CORP.'S announcement last week that it plans to buy Sun Microsystems Inc. raised questions about, well, almost every aspect of the blockbuster deal that would unite two Silicon Valley icons.

The only sure bets are that Oracle sees benefits in acquiring Java and the Solaris operating system — the only two Sun technologies mentioned as part of the announcement — and that thousands of additional Sun workers are likely to be laid off in order to meet Oracle's ambitious profit goals.

It's unclear, though, what will happen to the Java Community Process and Sun's other open-source technologies, such as the MySQL database. The same goes for the Sun-dominated OpenOffice.org application suite and its Sun-owned commercial cousin, StarOffice. Whether Oracle really intends to become a full-fledged hardware vendor and chip developer is also uncertain. Another question on the minds of Sun customers is how the deal with affect their service and support.

> **"The Solaris operating system is by far the best Unix technology available in the market.**
>
> **LARRY ELLISON,** CEO, ORACLE

In a brief conference call last Monday, Oracle CEO Larry Ellison outlined some of the reasons for the move and praised Java and Solaris — and largely left it at that. Ellison and other Oracle executives didn't take any questions about their plans, leaving the details to be spelled out at a later date.

And that leaves some Sun users worried about what the future may bring.

Among them is Alfonso Rivera, manager of network engineering at Embarq Corp., a telecommunications and Internet services provider in Overland Park, Kan. Sun's servers are generally more expensive than rival systems, Rivera said via e-mail. But, he added, the technology's reliability and Sun's "outstanding service and support practices more than offset the premium in hardware costs."

Now, Rivera said, he's concerned that Oracle will "undermine the Sun culture" and reduce the quality of customer service. If that happens, he said, the justification for paying Sun's premium prices will disappear.

Alex Wingeier, chief technical officer at CLR Choice Inc., a Palm Coast, Fla., company that has developed a real estate search engine, said that he and other members of his IT team also have concerns about Oracle taking over Sun.

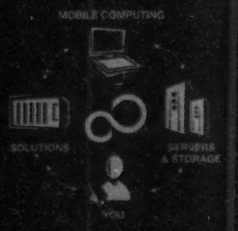
"We were not really keen on the fact that Oracle is buying Java, MySQL and OpenOffice," Wingeier said. "We worry that they quite possibly could stop internal development on either one."

That seems highly unlikely in the case of Java. During the conference call, Ellison described that technology as

Continued on page 12

Name: Kellee Carson
Drink: Soy Chai Latte
Job: IT Director, Produce Distributor

Fujitsu servers keep her data as fresh as her produce.



FUJITSU

In the produce business, freshness is everything. A little downtime can spoil a big shipment of bananas—or a major year-end report. That's why Kellee's business relies on reliable Fujitsu PRIMEQUEST® servers with Intel® Itanium® processors.

See how Fujitsu makes produce more productive at: www.fujitsudailyfuel.com

intel
Itanium inside
Mission Critical

© 2009 Fujitsu America, Inc. All rights reserved. Fujitsu and the Fujitsu logo are registered trademarks of Fujitsu Limited. PRIMEQUEST is a trademark of Fujitsu Limited in the United States and other countries. Intel, the Intel logo, Itanium and Itanium inside are trademarks of Intel Corporation in the United States and other countries. All other trademarks and product names are the property of their respective owners.

Microsoft Could Be a Winner in Oracle-Sun Deal

Microsoft Corp. has had few critics more vociferious than Oracle CEO Larry Ellison and Sun Chairman Scott McNealy. So with Oracle planning to acquire Sun, Microsoft should be worried, right?

Not necessarily.

If Oracle retools itself as a full-fledged systems vendor, as Ellison suggested that it might, hardware makers such as Dell Inc. and Hewlett-Packard Co. might cozy up more with Microsoft as a business partner.

HP and Oracle teamed up last year to roll out the jointly branded Database Machine and Exadata Storage Server, which combine Oracle's software and HP's ProLiant servers. Oracle is selling the systems, while HP handles delivery and services the hardware.

But Sanford C. Bernstein & Co. analyst Toni Sacconaghi wrote in a research note last week that HP "is likely to push alternatives to [Oracle] when possible, given that they are now direct competitors in the hardware space."

"The hardware business is king [for server vendors], and anything that threatens that becomes your mortal enemy," noted Miko Matsumura, a former Sun executive who is deputy chief technology officer at Software AG.

Some analysts expect Oracle to sell Sun's hardware business to a company such as Fujitsu Ltd., which makes Sparc-based systems. But Ellison, while not divulging any Sparc-related plans, said that the acquisition could enable Oracle to develop fully integrated systems.

– ROBERT McMILLAN AND AGAM SHAH OF THE IDG NEWS SERVICE

Oracle's DB Plus MySQL Don't Equal a Monopoly

Oracle's acquisition of Sun will bring together the world's leading relational database with the most popular open-source one – MySQL. But the deal isn't expected to draw the attention of antitrust regulators.

The acquisition would reduce competition "by removing the threat of MySQL 'going upmarket' from its base in Web applications" to take business from Oracle at the enterprise level, claimed Roger Burkhardt, CEO of Ingres Corp., an open-source database vendor. But even he acknowledged that the implications aren't strong enough to raise monopoly alarms.

Sun, which bought MySQL early last year, claims that the software has been downloaded more than 100 million times and that 12 million MySQL databases are in active use. Customers include companies such as Google and its YouTube unit, Craigslist, Yahoo, and Digg.

But the open-source database won't add much to Oracle's revenue: MySQL's sales amounted to just $38 million in 2007, putting it in 19th place among database vendors, according to market research firm IDC.

"MySQL has a tremendous impact, but it's in a piece of the market where no money changes hands," said John Newton, chief technology officer at Alfresco Software Inc., a vendor of open-source content management tools.

– ERIC LAI

Continued from page 10

"the single most important software asset we have ever acquired." He also said that Oracle's Java-based Fusion Middleware product line is the fastest-growing part of its business.

Essentially, Ellison boiled Sun down to two key assets: Java and Solaris. And if the Oracle CEO was going to thumb his nose at former Sun suitor IBM, one obvious way of doing that would be to talk up Solaris — which is exactly what Ellison did.

Many analysts didn't think that IBM, whose talks with Sun broke down three weeks ago, would have had any real interest in keeping Solaris alive on top of its own AIX version of Unix.

But Ellison claimed that Solaris is "by far the best Unix technology" and noted that Sun systems are the most popular platforms for running Oracle databases.

MUM ON SPARC, MYSQL

On the other hand, Ellison didn't make a long-term commitment to Sun's Sparc hardware, instead calling Solaris "the heart" of the company's server business.

In addition, he barely mentioned MySQL, a rival to Oracle's flagship database that Sun acquired last year. External predictions about MySQL's future are all over the map, with some observers saying it will thrive under Oracle and others expecting Ellison to throw it under the bus.

Not everyone is asking questions about the Oracle-Sun deal. Susan Walker, manager of enterprise computing services at St. Luke's Episcopal Health System in Houston, said she thinks it will "give new life to Sun" and pose increased competition for IBM in the enterprise IT market. Walker added that she hadn't had a good feeling about the prospect of IBM owning Sun.

But William Patterson, IT director at Nucor Steel Tuscaloosa Inc. in Alabama, said he's unsure about the future of technologies such as MySQL under Oracle's ownership. Patterson said that IBM would have been a better caretaker of Sun's software products and that combining their hardware technologies "would have definitely made more sense" than the Oracle deal.

One group that the acquisition is sure to be difficult for is Sun's workforce, which has already been hit hard by layoffs, including a planned cutback of up to 6,000 workers that was announced last November.

Sun lost $209 million in its second quarter, which ended in December, but it reported operating income of $114 million. Safra Catz, one of Oracle's two presidents, said during last week's conference call that the software vendor thinks it can run Sun at "substantially higher margins." She predicted that Sun will add more than $1.5 billion in operating profits during the first full fiscal year after the deal is completed and $2 billion the following year.

Much of the profit gains will come via layoffs, said Toni Sacconaghi, a financial analyst at Sanford C. Bernstein & Co. Sacconaghi had earlier forecast $800 million in operating profits during Sun's 2010 fiscal year, which is scheduled to start in July. Boosting profits to the level Oracle is shooting for, he said in a research note, will likely require cutting 5,500 to 10,000 more jobs at Sun. ■

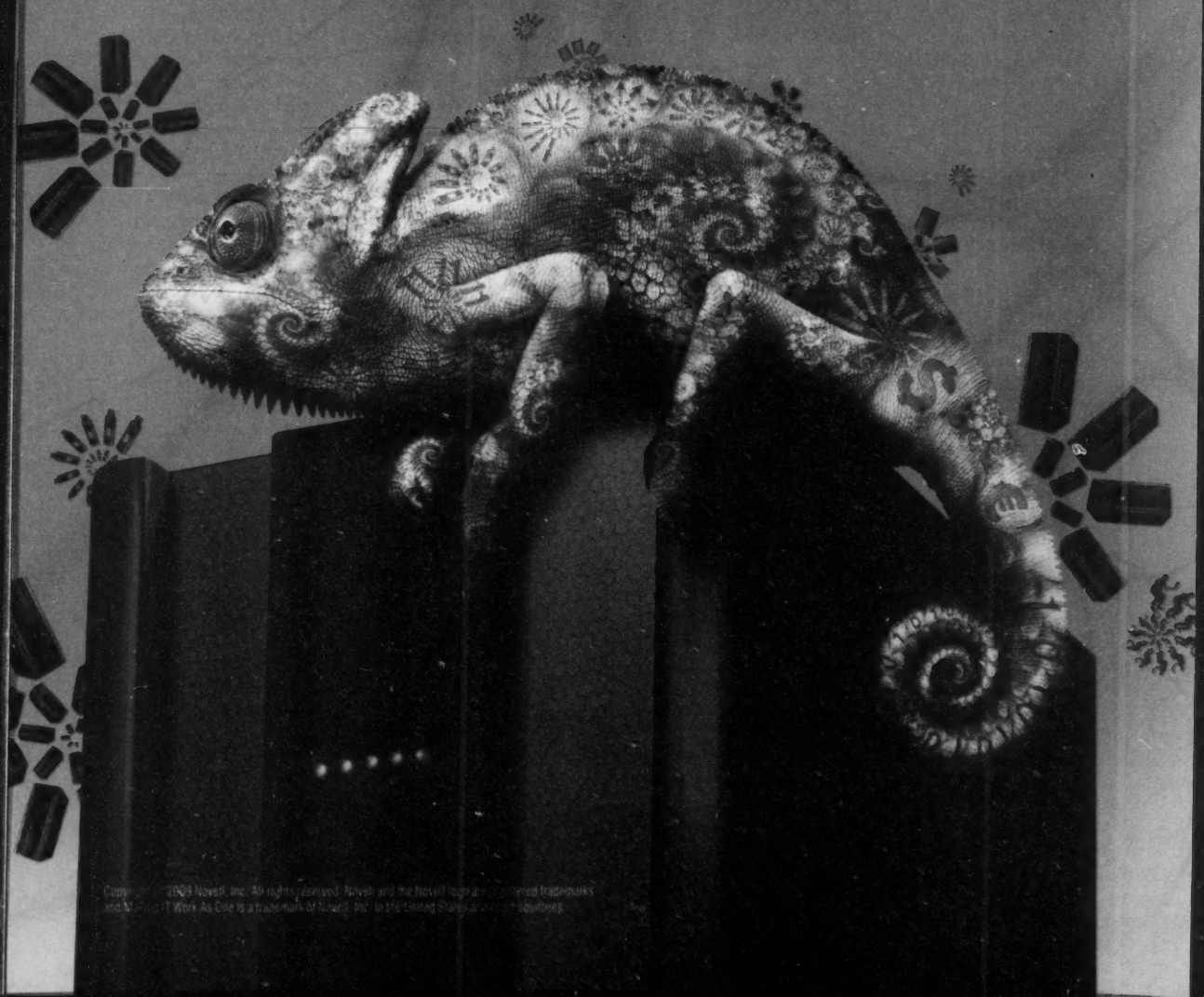
Robert McMillan *of the IDG News Service contributed to this story.*

Everything you need to sit on top of the mission-critical food chain.

Introducing the highly-evolved SUSE® Linux Enterprise 11. Today it's even more reliable, delivering high availability clustering with the affordability of open source. It's more interoperable, bridging your mixed Linux and Windows environments with support from both Novell® and Microsoft.® And it's more adaptable, powering your physical and virtual machines—from desktop to data center. All so you can lower your infrastructure costs, make your people more productive, and turn your organization's potential into reality. See how the evolution of Linux can make IT work as one for you.

novell.com/evolution

Novell®
Making IT Work As One™



Copyright © 2009 Novell, Inc. All rights reserved. Novell and the Novell logo are registered trademarks and Making IT Work As One is a trademark of Novell, Inc. in the United States and other countries.

IMAGE © FOTOLIA / SUPRIJONO SUHARJOTO

VMware Looks to Bring Data Centers Under the Cloud

It hopes its updated software will extend virtualization.

By James Niccolai

VMWARE INC. last week launched the long-awaited upgrade of its core virtualization software, which it calls a cloud operating system.

First touted by CEO Paul Maritz during VMware's user conference last fall, the new vSphere 4 software can transform data centers into "virtual compute clouds" in which applications move fluidly across computing, network and storage resources, company executives contended last week.

The hope, they said during a press conference at VMware's Palo Alto, Calif., headquarters, is that the upgrade will convince IT executives that virtualization is now reliable and scalable enough to run large corporate databases and other critical applications.

At the heart of VMware's promise to extend cloud computing to the data center are its claims that the software can now manage a cluster of computers with up to 32 physical servers, 2,048 processor cores and 32TB of memory. Perhaps more important for database applications, VMware said it has doubled the maximum number of I/O operations its software can perform to more than 200,000 per second.

Beyond the hype and bluster from executives at last week's announcement, some analysts and customers said that although some of VMware's claims are valid, the software still lacks some key features.

Chris Wolf, an analyst at Burton Group in Midvale, Utah, said that new processor technologies, combined with improvements in the virtualization software, will allow vSphere to run more-demanding applications.

However, Wolf added that VMware still doesn't offer tools that can provide all the management capabilities needed to treat a cluster of industry-standard servers as if it were a mainframe computer or a large Unix system. For example, VMware DRS, a tool that monitors processor and memory usage in a pool of servers to determine the most efficient platform available to run a virtual machine, still doesn't measure some key factors, like I/O utilization, he said.

And while Maritz last week talked about the danger of "lock-in" with proprietary systems from other vendors, vSphere still can't manage hypervisors from companies like Microsoft Corp. and Citrix Systems Inc. VMware executives argued that there isn't enough demand for those vendors' offerings to justify the investment required to support them, but some customers said they could use those capabilities today.

Christopher Rence, CIO at Fair Isaac Corp. (Fico), a Minneapolis-based provider of decision management tools and services, said his company has mostly standardized on VMware products but is also piloting Microsoft's Hyper-V virtualization technology and plans to use it for some applications. He noted that Fico must support the Microsoft offering because some of its customers run Hyper-V in their data centers. Thus, the ability to manage Hyper-V with vSphere would benefit the company.

Nonetheless, Rence said that VMware's technology has so far helped Fico consolidate 24 data centers into four. The company uses VMware widely in its development and testing processes and is now piloting some large database projects on vSphere, including applications that process up to 1,100 transactions per second.

Fico also uses a new technology in vSphere called vShield Zones to enforce security and compliance policies across a group of virtual machines. The technology makes it possible for virtual machines to maintain their security policies even if Fico moves them to a different cluster pool.

Other new features in vSphere 4 include fault-tolerance capabilities, support for thin storage provisioning — which allows less physical storage to be allocated to a virtual machine — the ability to switch an application between storage systems while the application is running, and a "distributed switch" developed with Cisco Systems Inc.

VSphere 4 is slated to be available later in the current quarter. Pricing ranges from $995 for a three-server package to $3,495 per processor for a high-end package called vSphere 4 Enterprise Plus.

Maritz said the low-end offering allows small companies to virtualize a pool of three or four servers so that a workload can fail over to a different system in the event of a hardware failure. ■

Niccolai *writes for the IDG News Service.*

SARA FORREST

■ THE GRILL

Gregg Favalora

The **optics pioneer** talks about **'crystal ball' 3-D imaging,** breakthrough **medical** applications, and **entrepreneurial** best practices.

Dossier

Name: Gregg Favalora

Title: Founder and chief technology officer

Organization: Actuality Medical Inc.

Location: Bedford, Mass.

Philosophy in a nutshell: "Hire people smarter than you are, and then get out of their way."

Favorite personality traits: Sincerity, humor and empathy

What he's reading: *House of Leaves*, by Mark Z. Danielewski

Most fascinating technology: Biologically inspired emergence

Dream dinner guests: "[Microcircuitry genius] Carver Mead, David Byrne, and my late grandfather, Irving Green, so he could see that his 'optics gene' passed on to me."

Your company has made some amazing advances in 3-D medical imaging. Can you talk specifically about your products and how the company's software developments help with patient care? We help doctors think and work better in 3-D. One product, Perspecta, is essentially a "crystal ball" that projects hologram-like images into true 3-D. It's been through several clinical studies for a common type of cancer treatment called external-beam radiation therapy. It does a great job helping doctors optimize their treatment plans.

Another effort is our work on a software system, PerspectaSeed, for prostate cancer treatment. Using a [traditional] display and ultrasound data from the operating room, our engineers are analyzing prostate imagery to train a computer to help doctors better place the 100 radioactive "seeds" used in prostate brachytherapy. This is a big deal. We believe we can radically decrease the side effects of common cancer treatments.

Which types of cancer are your products most successful in working with, and why is this technology superior to other types of 3-D imaging software? We believe

"We are inventing technologies to help doctors link their surgical plans to the actual shape of the tumors in the operating room.

that there is a lot of opportunity to help improve so-called soft-tissue cancer treatment, such as prostate, breast and liver cancer surgery.

Did you know that about half of all women who get a breast lump removed have to return because it turns out that the surgeon didn't get it all out the first time? Part of this is a visualization issue. We are inventing technologies to help doctors link their surgical plans to the actual shape of the tumors in the operating room. We hypothesize that this will result in saving hospitals money and that patients [will have] fewer side effects.

The device closely resembles a crystal ball. Is the image live? Can you move it around in real time on the screen while the patient is present? Our Perspecta product is an unusual type of display. The imagery it produces really is volume-filling, so you can walk all the way around it to inspect the 3-D scenes from any angle with your unaided eye. You can manipulate the image, say, to zoom in and out or figure out how one molecule could dock into another. The imagery is formed by projecting 6,000 patterns of light onto a special surface that rotates very rapidly. It took us several years to design the optics and software that makes it all happen. Gigabytes of data flow through the system every second, which, when we introduced it in 2001, was unusual. It is a 100 million-pixel display.

How does current technology limit what you're able to accomplish? I'm glad you asked that. 2009-era PCs are barely powerful enough to crunch large volumes of 3-D data at interactive rates. We've been dealing with this issue by using the PCs' video cards — GPUs — as inexpensive embedded parallel processors. Thanks to GPUs like the Nvidia GeForce 8800, we can slice and dice ultrasound and CT scan data in real time. However, we can certainly use even more power if it's provided. Likewise, our holographic video displays will improve as digital light modulators, like the Texas Instruments DLP technology, become faster.

What is the next big leap for medical technology in general? I hope to see major advances in the fields of medical imaging at the molecular level, microscopic endoscopy [enabling "virtual pathology" in the operating room] so that the surgeon knows where to snip, and improvements in electronic medical records. Hospitals are fairly siloed, so that is really challenging.

Also, frankly, I am learning a big lesson about how some hospitals operate, which is that the money-making treatment products are adopted with a higher priority than what's necessarily best for the patient. I wish that wasn't so.

What are some of the obstacles you face with running a start-up in such a competitive industry? Fortunately, we are the only company in the world selling volumetric 3-D displays. We face a bigger challenge in our medical device/software work, where we're up against the global medical players. We maintain an aggressive patent portfolio, hire very bright people and make sure our engineers spend plenty of time watching cases in the OR so we build things our customers will find useful.

Right now, we're trying to crack a 10-year-old problem of detecting metallic seeds in prostate patients, and I feel really good that our contrarian solution will be a winner. We'll know very soon.

Do you find it challenging to be both a businessman and an optical engineer? Yes, that's tugged at me for a while. Although I have entrepreneurial DNA, there are times when I prefer to be in the lab or at my notebook doing R&D. Also, young entrepreneurs take an unusual career risk of "leapfrogging" over the traditional apprenticeship path; instead, we manage teams of brilliant people who do things we've never personally done.

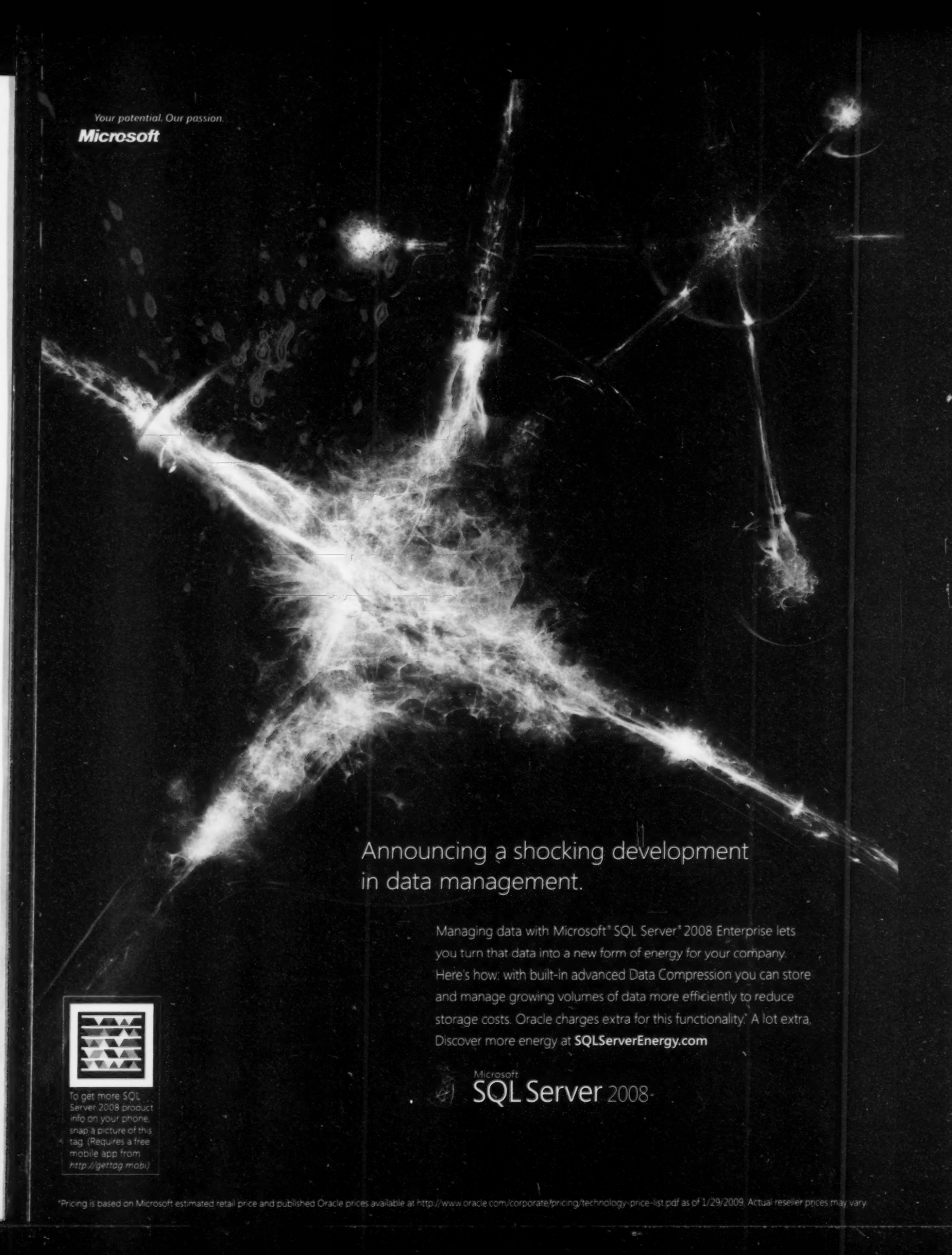
I do think it's valuable that seeing the business side informs the engineering effort, and vice versa.

What advice do you have for other aspiring young innovators? I love the feelings of solving engineering problems and achieving big milestones, but for some reason, my brain always ratchets to the next difficulty-goal level before I have a chance to enjoy what we've accomplished.

Advice? Talk to real customers, in person, starting as early in the game as possible. Find a great mentor. Get involved in the local start-up scene, being sure to give of your time as well. Patent like crazy. Seek personal referrals to the best people. Take risks, but not with your family's well-being.

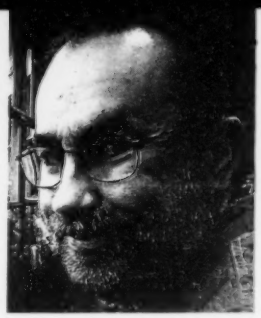
And as my chairman, Rob Ryan [founder of Ascend Communications], taught me when I didn't think there were enough hours in the day, "Gregg, there are plenty of hours from 5 to 9."

— Interview by **Sara Forrest**, *a freelance photographer and writer in New York (saraforrestphoto@gmail.com)*


Your potential. Our passion.
Microsoft
Announcing a shocking development in data management.
Managing data with Microsoft® SQL Server® 2008 Enterprise lets you turn that data into a new form of energy for your company. Here's how: with built-in advanced Data Compression you can store and manage growing volumes of data more efficiently to reduce storage costs. Oracle charges extra for this functionality.* A lot extra. Discover more energy at SQLServerEnergy.com
Microsoft SQL Server 2008
To get more SQL Server 2008 product info on your phone, snap a picture of this tag. (Requires a free mobile app from http://gettag.mobi)
*Pricing is based on Microsoft estimated retail price and published Oracle prices available at http://www.oracle.com/corporate/pricing/technology-price-list.pdf as of 1/29/2009. Actual reseller prices may vary.

■ OPINION

Steven J. Vaughan-Nichols



Microsoft Is Doing Something Half Right

EVER SINCE Bill Gates stepped down and Steve Ballmer took over his role, Microsoft has been getting one thing after another wrong. Vista continues to be a disaster both for users and for the company's bottom line. And Microsoft's ad campaign last year, starring Gates and Jerry Seinfeld, is already a model of how *not* to do television advertising. Somehow, though, after years of stumbling around like a drunken college freshman after an NCAA basketball win, Microsoft is getting its act together.

First, Microsoft has reluctantly — oh how reluctantly — brought back Windows XP. Officially, Microsoft has cut XP support. Unofficially, hardware vendors such as Hewlett-Packard aren't going to let XP die anytime soon. You'll still be getting new PCs with XP on them well into 2010, and I wouldn't be surprised to see fresh copies of XP appearing in 2011.

Microsoft finally got it. No one with two brain cells wants Vista.

What's more amazing to me, though, is that Microsoft finally figured out that after Vista, no one wants a long, drawn-out rollout of a new Windows operating system. So, instead of orchestrating its traditional years-long series of preannouncements and announcements, Microsoft is just focusing on getting Windows 7 — a.k.a. Vista Lite — out as fast as possible, with as little official fanfare as possible.

That doesn't mean Microsoft hasn't been advertising Windows 7. But buying time on television and space in magazines might make more people realize just how thoroughly Microsoft has given up on Vista. Instead, Microsoft is "advertising" the upcoming release by leaking betas of Windows 7 almost every week — and will soon do the same with release-candidate builds.

■ As long as you don't look too closely at Microsoft's offerings, its new marketing and ads are making Windows look good again.

It's funny that some people actually think that anyone is "pirating" Windows 7 betas. It's clear that Microsoft is deliberately leaking them to build up buzz around the new operating system. Don't believe me? Then why does Microsoft give away free authentication keys that will let *any* copy of Windows 7 work? If the company didn't want those copies of Windows 7 out there, it wouldn't do that. This tactic is fairly subtle: By making people work — but not too hard — to get copies of Windows 7, Microsoft is leading them to believe that they're onto something special. And since it has been a long, long time since anyone thought there was something special about Windows, this is savvy marketing on Microsoft's part.

(Mind you, I've been running Windows 7 for quite some time now on a variety of test boxes, and it's not all that great. It's better than Vista, but that's really not saying much. For my money, XP SP3 is still the best of the Windows family.)

Finally, Microsoft has also come up with a winning set of TV ads. The ones with the cute kids are, well, cute, and the Mac attack ads do make the point that PCs really are cheaper than Apple's proprietary hardware. However, if you're a thinking user, you'll realize that you get what you pay for and that Macs really are better than low-cost PCs. And if you're a thinking user who wants a really low-cost PC, you don't want Windows anyway — you want desktop Linux.

But Microsoft's ads aren't meant for savvy computer users. They're meant for home users with XP Home and Conficker on their PCs. As long as you don't look too closely at Microsoft's offerings, its new marketing and ads are making Windows look good again. Who would have thought that Microsoft could pull the wool over even dumb users' eyes again? That, nevertheless, is what it's managing to do. ■

Steven J. Vaughan-Nichols *has been writing about technology and the business of technology since CP/M-80 was cutting-edge and 300bit/sec. was a fast Internet connection — and we liked it! He can be reached at sjvn@vnal.com.*

Attend the world's largest event for storage, data center, infrastructure, and business continuity.

At SNW, you can choose from over 150 educational sessions and network with peers from around the globe, plus visit with top solutions providers in the world's largest Expo devoted to storage and related technologies. This is your opportunity to quickly gather reliable, firsthand, practical knowledge you can put to work right away.

SNW is where you can learn, share experiences and make decisions. Join your peers and industry experts this October in Phoenix!

COMPUTERWORLD SNIA

SNW

October 12-15, 2009
JW Marriott Desert Ridge, Phoenix, Arizona
www.snwusa.com

SPECIAL REPORT

INTERNET WARFARE: Are We Focusing on the

A CRYSTAL-CLEAR denouement of U.S readiness to combat threats in cyberspace came at a hearing held March 10 by the U.S. House Committee on Homeland Security. After about an hour of listening to testimony from five witnesses representing government and the private sector, committee chairman Rep. Bennie Thompson (D-Miss.) asked if any of them felt that the federal government was prepared to deal with a cybercatastrophe. Not one did.

More than seven years after the terrorist attacks of Sept. 11, 2001, there's widespread consensus that federal efforts to secure cyberinfrastructure

ILLUSTRATION: ANASTASIA VASILAKIS

A lack of vision and leadership have left the U.S. woefully unprepared for a cybercatastrophe. By Jaikumar Vijayan

Wrong Things?

are bogged down by a lack of vision, planning and leadership. While the government has struggled to come up with a cohesive national strategy for defending its interests on the Internet, menaces in cyberspace have continued to grow and today pose a grave threat to national and economic security.

Adversaries — which include unfriendly governments and militaries, intelligence agencies, organized criminals, and hactivists — have by most accounts already penetrated U.S government and private networks or are actively engaged in doing so.

Most of the efforts are focused on pilfering secrets from public and private IT organizations and appear to be profit- or espionage-related. A report released in March by the University of Toronto and think tank The SecDev Group showed how a group with apparent ties to China has methodically breached systems in more than 100 countries, apparently for espionage purposes. At the same time, the potential for attackers to disrupt vital networks and systems in critical infrastructure areas such as banking and power is growing daily.

The threat has not gone unnoticed. Earlier this month, Sens. Olympia Snowe (R-Maine) and Jay Rockefeller (D-W.Va.) introduced legislation that would give the federal government sweeping cybersecurity authority.

Coverage continues next week with "Internet Warfare: Where Are We Most Vulnerable?"

The legislation would give the government a more direct role in developing and enforcing baseline standards, not just for public agencies but also for companies in critical infrastructure areas such as financial services, utilities and health care. It would empower the president to declare a cyber-emergency if needed and allow him to disconnect federal or private-sector networks in the interest of national security.

The current administration has made cybersecurity a priority. In February, President Barack Obama enlisted Melissa Hathaway, a Bush administration official who is credited with helping to develop a multibillion-dollar classified initiative aimed at better securing federal systems, to conduct a 60-day review of the government's cybersecurity efforts.

Hathaway's report and any strategies and policies that result from its findings are going to be critical in the near and long terms. "Our digital infrastructure has become the most important underpinning of U.S. national and economic security," says Amit Yoran, former director of the National Cybersecurity Division at the U.S. Department of Homeland Security (DHS). "In order to make good resource-allocation decisions, we need to understand the risk better."

SPECIAL REPORT

INTERNET WARFARE: Are We Focusing on the

A CRYSTAL-CLEAR denouement of U.S readiness to combat threats in cyberspace came at a hearing held March 10 by the U.S. House Committee on Homeland Security. After about an hour of listening to testimony from five witnesses representing government and the private sector, committee chairman Rep. Bennie Thompson (D-Miss.) asked if any of them felt that the federal government was prepared to deal with a cybercatastrophe. Not one did.

More than seven years after the terrorist attacks of Sept. 11, 2001, there's widespread consensus that federal efforts to secure cyberinfrastructure

ILLUSTRATION: ANASTASIA VASILAKIS

A lack of vision and leadership have left the U.S. woefully unprepared for a cybercatastrophe. By Jaikumar Vijayan

Wrong Things?

are bogged down by a lack of vision, planning and leadership. While the government has struggled to come up with a cohesive national strategy for defending its interests on the Internet, menaces in cyberspace have continued to grow and today pose a grave threat to national and economic security.

Adversaries — which include unfriendly governments and militaries, intelligence agencies, organized criminals, and hactivists — have by most accounts already penetrated U.S government and private networks or are actively engaged in doing so.

Most of the efforts are focused on pilfering secrets from public and private IT organizations and appear to be profit- or espionage-related. A report released in March by the University of Toronto and think tank The SecDev Group showed how a group with apparent ties to China has methodically breached systems in more than 100 countries, apparently for espionage purposes. At the same time, the potential for attackers to disrupt vital networks and systems in critical infrastructure areas such as banking and power is growing daily.

The threat has not gone unnoticed. Earlier this month, Sens. Olympia Snowe (R-Maine) and Jay Rockefeller (D-W.Va.) introduced legislation that would give the federal government sweeping cybersecurity authority.

Coverage continues next week with "Internet Warfare: Where Are We Most Vulnerable?"

The legislation would give the government a more direct role in developing and enforcing baseline standards, not just for public agencies but also for companies in critical infrastructure areas such as financial services, utilities and health care. It would empower the president to declare a cyber-emergency if needed and allow him to disconnect federal or private-sector networks in the interest of national security.

The current administration has made cybersecurity a priority. In February, President Barack Obama enlisted Melissa Hathaway, a Bush administration official who is credited with helping to develop a multibillion-dollar classified initiative aimed at better securing federal systems, to conduct a 60-day review of the government's cybersecurity efforts.

Hathaway's report and any strategies and policies that result from its findings are going to be critical in the near and long terms. "Our digital infrastructure has become the most important underpinning of U.S. national and economic security," says Amit Yoran, former director of the National Cybersecurity Division at the U.S. Department of Homeland Security (DHS). "In order to make good resource-allocation decisions, we need to understand the risk better."

WHY PREVIOUS POLICIES FAILED

President Barack Obama has promised to make cybersecurity a top priority. In a January report, Forrester Research Inc. analyst Khalid Kark examined why the previous administration's policies were "outdated and not in line with the realities of today's complex and targeted threats" and found the following problems:

- **Lack of leadership.** The idea of a cybersecurity czar reporting up to the president sounds good, but the previous three people in this position did not last very long. The last was Richard Clark, who was the special adviser to the president on cybersecurity. The U.S. government hasn't had a clear leader in that position since 2003.

- **Lack of coordination among agencies.** Federal agencies are operating in their own silos, with limited coordination and communication among them. It is generally assumed that the Department of Homeland Security has the mandate to run cross-industry cybersecurity initiatives, but in reality, the DHS has trouble coordinating its own internal efforts.

- **No input from the private sector.** The strategy for cybersecurity has been developed primarily by the intelligence community within the U.S. government, which has a very different perspective than the commercial sector. The private sector should not only be at the table, but in many cases, it should also be leading the discussions and developing solutions that can be applied in both the private and public sectors.

- **Lack of information-sharing.** Government cybersecurity initiatives have largely been isolated from the private sector. Many assessments and initiatives are classified and can't be shared with the private sector, which could provide valuable input and even help in the execution of some of those activities.

According to Yoran and several other experts in industry and government, the feds need to do the following key things in the near term.

IMPLEMENT STRONG LEADERSHIP

If the national information security agenda seems like a ship adrift on the high seas, security executives and analysts say that's because there's no one at the helm — or at least no one who has been truly capable of enforcing the order needed to steer a steady course.

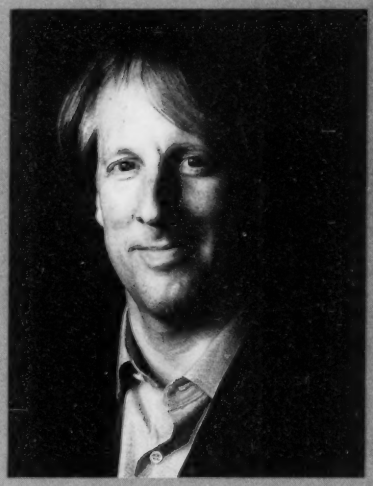
On paper at least, the DHS is responsible for overseeing information security across the federal government. But for most of its existence, the agency's leadership on such issues has been conspicuous by its absence. Even where it has tried, its efforts have been less than successful.

The National Cyber Security Center (NCSC), which was set up within the DHS in January 2008 with the specific task of coordinating information security across the federal government, has so far failed to get off the ground. In March, its first director, Rod Beckström, quit the post after just a year on the job, citing a lack of support from within the DHS and turf wars with the National Security Agency.

At the time Beckström quit, the NCSC had almost no funding for its task, just two employees and two "detailees" from the NSA. "If you are going to run a major coordination effort, you've got to have the resources to build that capability," Beckström said at the time, adding that "the financial constraints which have been placed upon the NCSC are simply ridiculous and leave the nation vulnerable to attack."

The NSA, which is in charge of the Comprehensive National Cybersecurity Initiative (CNCI), has been jostling for broader control of the federal information security agenda. But while almost everyone acknowledges that the NSA can bring the skills, experience and clout needed to do the job, the prospect of a spy agency running the domestic cyberagenda does not sit well with security watchdogs.

Rather, the role of setting, overseeing and coordinating a national information security agenda should rest directly with the White House, according to the Center for Strategic and International Studies (CSIS), a bipartisan Washington think tank, and other organizations. Then the DHS and other federal agencies could work with a White House office of cyberspace to roll out and manage security policies.



"The financial constraints which have been placed upon the NCSC are simply ridiculous and leave the nation vulnerable to attack."

ROD BECKSTRÖM, FORMER DIRECTOR, NATIONAL CYBER SECURITY CENTER

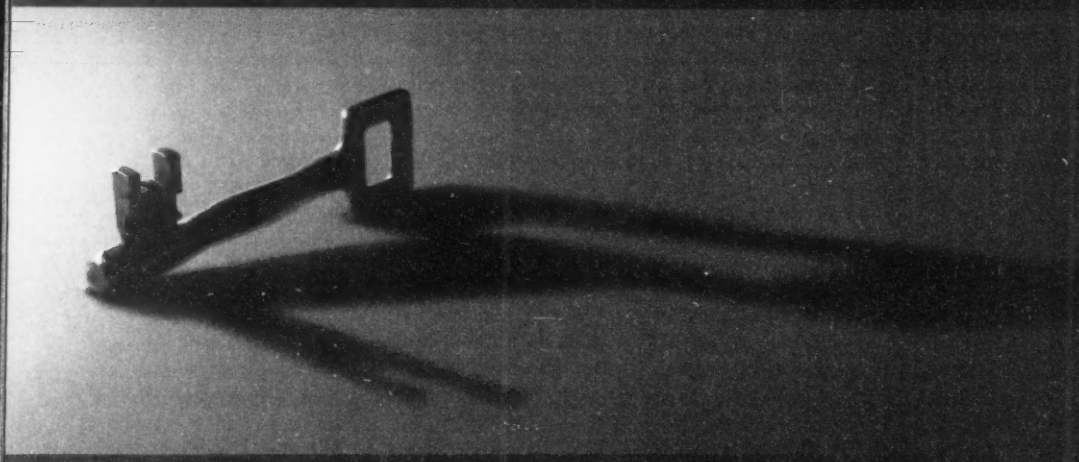
Unlike the DHS, "the White House has the authority to make agencies act,' " says Gregory Wilshusen, director of information security issues at the U.S. Government Accountability Office. Establishing White House responsibility would ensure that stakeholders cooperated in marshaling the resources needed to implement a national cyberstrategy, he says.

CREATE A NATIONAL STRATEGY FOR DEFENDING CYBERSPACE

Over the past few years, billions of dollars have been poured into cybersecurity across the federal government. The investments have yielded numerous scattershot efforts, such as a rollout of smart ID cards across federal agencies, a governmentwide move to more-secure Internet

Continued on page 24

YOU DON'T NEED MORE SECURITY. YOU NEED BETTER SECURITY.



CA Security Management software streamlines your IT security environment so your business can be more secure, agile and compliant without upsizing your infrastructure. All with faster time to value. Greater efficiency starts with more efficient IT. That's the power of lean.

Learn more at ca.com/security

Copyright © 2009 CA. All rights reserved.

ca Software

HOW THE NEW POLICIES WILL DIFFER

The specifics of the Obama administration's cybersecurity strategy are still to be determined, but Forrester analyst Khalid Kark says that early indications suggest that it plans radical changes such as these:

- **The appointment of a cybersecurity czar. This person will coordinate and communicate governmentwide initiatives and be accountable for ensuring the protection of the public and private infrastructures that are necessary for a thriving economy.**
- **Focus on commercial information assets. One of the major battlegrounds in the era of cyberwarfare will be private-sector information assets and intellectual property. Despite a number of cyberattacks on major U.S. companies that can be traced to foreign countries, the government hasn't undertaken a concerted effort to protect private-sector information assets.**
- **Expansion of cybersecurity efforts to other federal agencies. While the U.S. government takes pride in the way it protects its military and intelligence assets, it lacks a similar focus on protecting information within other departments against a coordinated foreign attack. The new administration is expected to make other commercially sensitive agencies, such as the Commerce Department, a focal point of data protection efforts.**
- **Funding for security research and development efforts. Government security initiatives have been largely reactive so far. The private sector funds projects with established ROIs. An initiative may not have a solid business case, but if the case for safeguarding sensitive commercial and government targets is compelling, the effort should be funded by the government. The new administration has promised to do that.**

Continued from page 22

protocols and the highly classified CNCI to boost the ability of government to detect and respond to threats and security vulnerabilities in near real time.

The initiatives are expected to yield significant benefits down the road, but none of them is tied to any broader strategic goals or missions. One of the most pressing needs is for a comprehensive national security strategy that sets the agenda for how, where, when and why security investments need to be made and who will be responsible for such initiatives. The strategy will need to spell out baseline standards for entities in critical infrastructure areas.

The CSIS, which in December submitted a set of security recommendations to President Obama, argues that such a strategy would require the government to declare its cyberinfrastructure a vital asset for national and economic security. It would then need to indicate its willingness to use all of the tools at its disposal — including diplomatic, economic, military and intelligence capabilities — to protect that asset.

BUILD A CYBER-RESPONSE CAPABILITY

In 1963, soon after the Cuban Missile Crisis, President John F. Kennedy established the National Communications System. Its task was to work with federal agencies and private industry to ensure the reliability and availability of telecommunications systems during emergencies. During the 9/11 crisis, the NCS played a crucial role in coordinating the resources needed to ensure that vital communication services remained uninterrupted.

When it comes to cybersecurity, there is no equivalent capability, says James Lewis, director of the technology and public policy program at the CSIS. "If there's a fire on the Internet, who's the fire department?" he asks. In the event of an Internet crisis, there is no single entity that either the federal government or private industry can depend on to coordinate a response. "There's no one you can simply pick up the phone and speak with," Lewis says.

Implementing such a capability is not going to be easy, says Paul Kurtz, former special assistant to President Bush and former senior director for critical infrastructure protection on the White House's Homeland Security Council. Attacks against key Internet protocols and routing technologies could cause considerable and lengthy disruption. Coordinating a response could involve numerous stakeholders, including carriers, Internet service providers, technology vendors and bodies like the Internet Corporation for Assigned Names and Numbers, says Kurtz, who is currently a partner at Good Harbor Consulting LLC.

> **"If there's a fire on the Internet, who's the fire department?"**
>
> JAMES LEWIS, DIRECTOR, TECHNOLOGY AND PUBLIC POLICY PROGRAM, CSIS

"In the old days, we had trucks with SS7 network switches on them that could be rolled in place quickly to reconnect copper networks," Kurtz says. "In an IP-based world, we have not even begun to scratch the surface of how we would restore networks."

SECURE TARGETS IN CRITICAL INFRASTRUCTURE AREAS

A "digital Pearl Harbor," in which adversaries take down large swaths of the Internet, is a possibility that needs to be prepared for, security analysts say. But far more likely, and of greater concern, are more-focused attacks against critical infrastructure targets such as the power grid, water supplies and financial services institutions.

The blackout in the Northeast in 2003 remains a potent example of the havoc a computer failure can cause — even if, as was the case then, the incident is caused by negligence rather than malice.

Another reminder is an experiment conducted in March 2007 in which the Idaho National Laboratory showed how it could reduce a power turbine to a smoking, shuddering, metal-spewing mess simply by executing malicious code on the computer controlling the system.

These examples are only the tip of the iceberg. According to the GAO's Wilshusen, the trend over the past few

Continued on page 26

HOW THE NEW POLICIES WILL DIFFER

The specifics of the Obama administration's cybersecurity strategy are still to be determined, but Forrester analyst Khalid Kark says that early indications suggest that it plans radical changes such as these:

- **The appointment of a cybersecurity czar.** This person will coordinate and communicate governmentwide initiatives and be accountable for ensuring the protection of the public and private infrastructures that are necessary for a thriving economy.

- **Focus on commercial information assets.** One of the major battlegrounds in the era of cyberwarfare will be private-sector information assets and intellectual property. Despite a number of cyberattacks on major U.S. companies that can be traced to foreign countries, the government hasn't undertaken a concerted effort to protect private-sector information assets.

- **Expansion of cybersecurity efforts to other federal agencies.** While the U.S. government takes pride in the way it protects its military and intelligence assets, it lacks a similar focus on protecting information within other departments against a coordinated foreign attack. The new administration is expected to make other commercially sensitive agencies, such as the Commerce Department, a focal point of data protection efforts.

- **Funding for security research and development efforts.** Government security initiatives have been largely reactive so far. The private sector funds projects with established ROIs. An initiative may not have a solid business case, but if the case for safeguarding sensitive commercial and government targets is compelling, the effort should be funded by the government. The new administration has promised to do that.

Continued from page 22

protocols and the highly classified CNCI to boost the ability of government to detect and respond to threats and security vulnerabilities in near real time.

The initiatives are expected to yield significant benefits down the road, but none of them is tied to any broader strategic goals or missions. One of the most pressing needs is for a comprehensive national security strategy that sets the agenda for how, where, when and why security investments need to be made and who will be responsible for such initiatives. The strategy will need to spell out baseline standards for entities in critical infrastructure areas.

The CSIS, which in December submitted a set of security recommendations to President Obama, argues that such a strategy would require the government to declare its cyberinfrastructure a vital asset for national and economic security. It would then need to indicate its willingness to use all of the tools at its disposal — including diplomatic, economic, military and intelligence capabilities — to protect that asset.

BUILD A CYBER-RESPONSE CAPABILITY

In 1963, soon after the Cuban Missile Crisis, President John F. Kennedy established the National Communications System. Its task was to work with federal agencies and private industry to ensure the reliability and availability of telecommunications systems during emergencies. During the 9/11 crisis, the NCS played a crucial role in coordinating the resources needed to ensure that vital communication services remained uninterrupted.

When it comes to cybersecurity, there is no equivalent capability, says James Lewis, director of the technology and public policy program at the CSIS. "If there's a fire on the Internet, who's the fire department?" he asks. In the event of an Internet crisis, there is no single entity that either the federal government or private industry can depend on to coordinate a response. "There's no one you can simply pick up the phone and speak with," Lewis says.

Implementing such a capability is not going to be easy, says Paul Kurtz, former special assistant to President Bush and former senior director for critical infrastructure protection on the White House's Homeland Security Council. Attacks against key Internet protocols and routing technologies could cause considerable and lengthy disruption. Coordinating a response could involve numerous stakeholders, including carriers, Internet service providers, technology vendors and bodies like the Internet Corporation for Assigned Names and Numbers, says Kurtz, who is currently a partner at Good Harbor Consulting LLC.

> **"If there's a fire on the Internet, who's the fire department?"**
> JAMES LEWIS, DIRECTOR, TECHNOLOGY AND PUBLIC POLICY PROGRAM, CSIS

"In the old days, we had trucks with SS7 network switches on them that could be rolled in place quickly to reconnect copper networks," Kurtz says. "In an IP-based world, we have not even begun to scratch the surface of how we would restore networks."

SECURE TARGETS IN CRITICAL INFRASTRUCTURE AREAS

A "digital Pearl Harbor," in which adversaries take down large swaths of the Internet, is a possibility that needs to be prepared for, security analysts say. But far more likely, and of greater concern, are more-focused attacks against critical infrastructure targets such as the power grid, water supplies and financial services institutions.

The blackout in the Northeast in 2003 remains a potent example of the havoc a computer failure can cause — even if, as was the case then, the incident is caused by negligence rather than malice.

Another reminder is an experiment conducted in March 2007 in which the Idaho National Laboratory showed how it could reduce a power turbine to a smoking, shuddering, metal-spewing mess simply by executing malicious code on the computer controlling the system.

These examples are only the tip of the iceberg. According to the GAO's Wilshusen, the trend over the past few

Continued on page 26

Join us in the Inner Circle.

The Computerworld Inner Circle Research Panel was established as a way for members of the IT community to share information and gain insight into various technology topics, including new initiatives and top issues faced by IT professionals and executives.

Inner Circle panel members get exclusive access to results of the surveys on the panel site at: **www.computerworldinnercircle.com**, and are eligible for some nice cash and prize giveaways for their participation. We look forward to hearing your input!

Join for Free!

To register as a panel member, visit **www.computerworld.com/haic**

COMPUTERWORLD
INNER CIRCLE
RESEARCH PANEL

Continued from page 24

years to connect the systems that are used to control critical equipment to the Internet — in power generation and distribution, water treatment, biotech, pharmaceuticals and transportation — is making them more vulnerable to threats.

This was demonstrated in 2000, Wilshusen says, when a disgruntled employee at an Australian water-treatment plant released about 264,000 gallons of raw sewage into nearby rivers and parks by using a radio transmitter to break into the control systems.

In August 2003, a computer virus called Sobig managed to infiltrate a control system at CSX Corp.'s headquarters in Florida and shut down railroad signaling systems up and down the East Coast for hours, he says.

And in October 2006, a foreign hacker broke into a system at a water filtration plant in Harrisburg, Pa., after an employee's laptop computer was compromised via the Internet and then used as an entry point to install malware on the plant's computer system.

Although almost all critical infrastructure systems are owned by the private sector, making sure they are adequately protected should be a government priority, says Wilshusen. Not only should baseline security standards be established for critical infrastructure industries, he says, but there should also be regulations for enforcing them and a strategy for sharing information about security practices and other matters between the private and public sectors.

USE FEDERAL PROCUREMENT POWER TO FORCE BETTER SECURITY FROM VENDORS

Having served as the de facto CIO of the federal government under the Bush administration, Karen Evans knows a lot about how to use the government's enormous buying power to force technology vendors to improve security. "When you spend $71 billion in the marketplace, you should be very clear about what your requirements are" and expect vendors to abide by them, she says.

One place where the government has successfully done this is under the Federal Desktop Core Configuration (FDCC) initiative, in which it is working with Microsoft Corp. and other technology vendors to ensure that all Windows XP and Vista desktops delivered to the government have standard baseline security configurations. Evans says there's no reason why a similar model can't be implemented to also get other vendors to do things such as turn off default configurations and disable functions that create security risks before products are delivered to agencies. Implementing security language in federal acquisition rules is much easier than forcing regulations down vendors' throats, she says.

Requiring vendors to bake in security and centralizing procurement across the government could also bring costs down significantly, says Alan Paller, director of research at the SANS Institute, a training and certification organization in Bethesda, Md. "Right now, there's enormous inefficiency" when it comes to security purchases, he says.

DEVELOP AN OFFENSIVE CAPABILITY

Patti Titus, the former chief information security officer at the Transportation Security Administration, is among a growing number of executives arguing for the development of deterrent capabilities in cyberspace. "What we need to say is, 'We are the U.S., and if you mess with us, you'd better be careful,' " says Titus, who is currently chief information security officer at Unisys Corp.

For too long, the country has been focusing on building a defensive capability that has done little to stop adversaries from infiltrating government networks and supply chain and distribution systems, she says. "It's time to come up with some way of launching back at those that mean to do harm," Titus suggests.

But figuring out the nuances of such a strategy can be tricky, says Kurtz. "There is some real work that needs to be done" on a global basis to think through such issues, he says. "What is an act of war in cyberspace? We need to have a far more substantial dialogue here in the United States and abroad about what this means," he says, especially because the means to do harm in cyberspace are not restricted to governments and militaries.

> **"It's time to come up with some way of launching back at those that mean to do harm.**
>
> PATTI TITUS, CHIEF INFORMATION SECURITY OFFICER, UNISYS CORP.

> **"Determining who ... the enemies are is one of the biggest problems we have.**
>
> SHAWN CARPENTER, FORMER NETWORK SECURITY ANALYST, SANDIA NATIONAL LABORATORIES

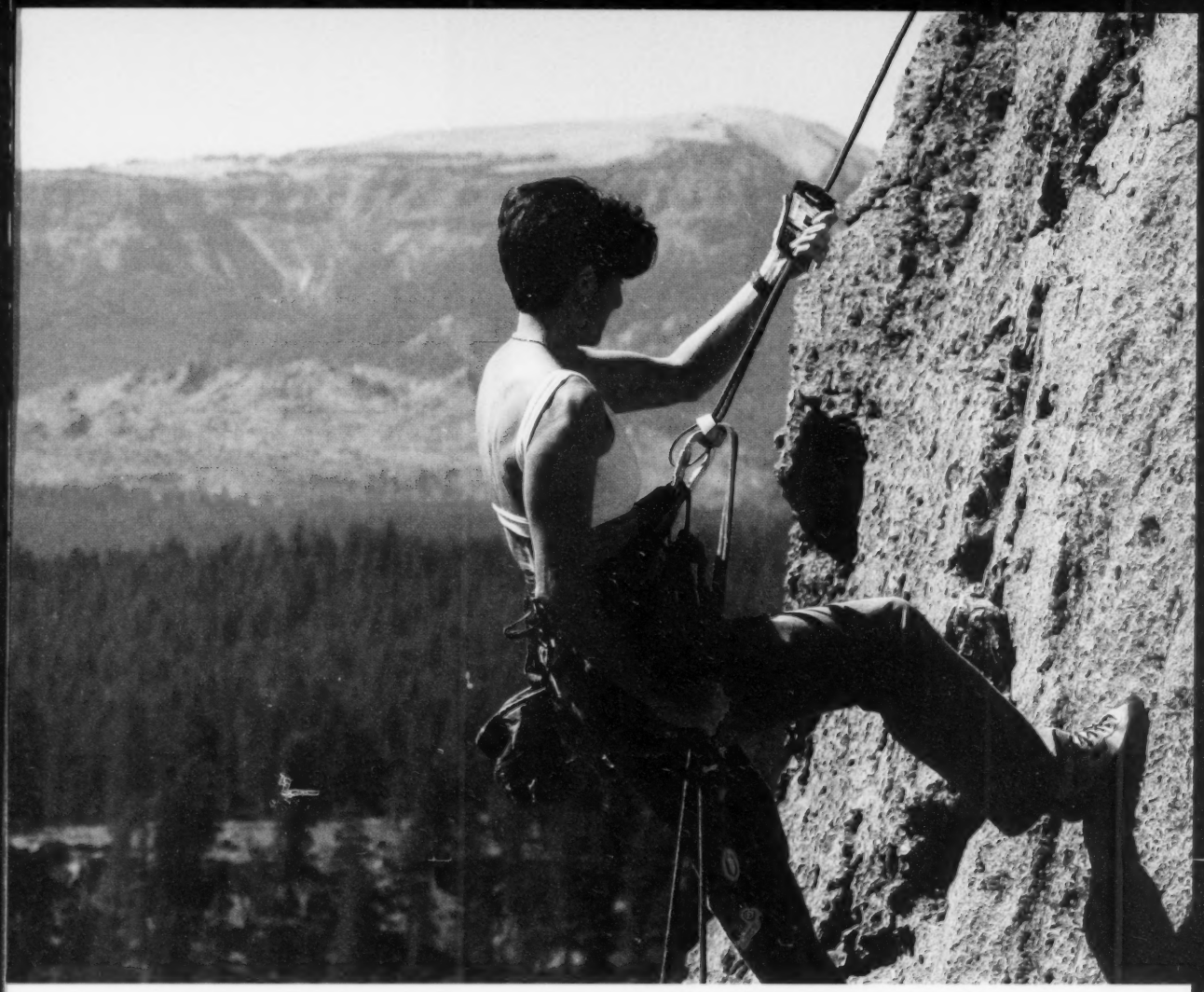
Countries don't brag about their cyberoffensive capabilities the way they might "display fighter planes and battleships," says Steven Chabinsky, senior cyber adviser to the director of national intelligence. "They guard them in a very secretive manner," and there's no telling if they intend to use their cyberweapons, says Chabinsky. "In cyber, capabilities tend to get better over time, and intentions can change quickly," he cautions. And there is always the possibility that a nation that wants to do damage can simply hijack or use capabilities built by others.

"Determining who the attackers are, who the enemies are, is one of the biggest problems we have as a government and in the private sector," says Shawn Carpenter, a former network security analyst at Sandia National Laboratories.

Carpenter was fired in January 2005 for his independent probe of a network security breach at the government research facility — an undertaking in which he did some reverse-hacking and traced the incident back to a Chinese espionage group called Titan Rain. Make no mistake, he says, the enemy is already here, lurking in sensitive systems and networks — in control of large botnets that are inside financial systems and the power grid — and it needs to be stopped.

"My definition of a digital Pearl Harbor is where these people are already here," he says. "They already have access and are just sort of hanging out maintaining their access for the time when they get some instruction to bring down the system or corrupt information." ■

Don Tennant *contributed to this report.*



Anywhere. Anytime.

Can't get enough of Computerworld?
No matter where you are, Computerworld is there.
Keep up with the latest technology news on your PDA.

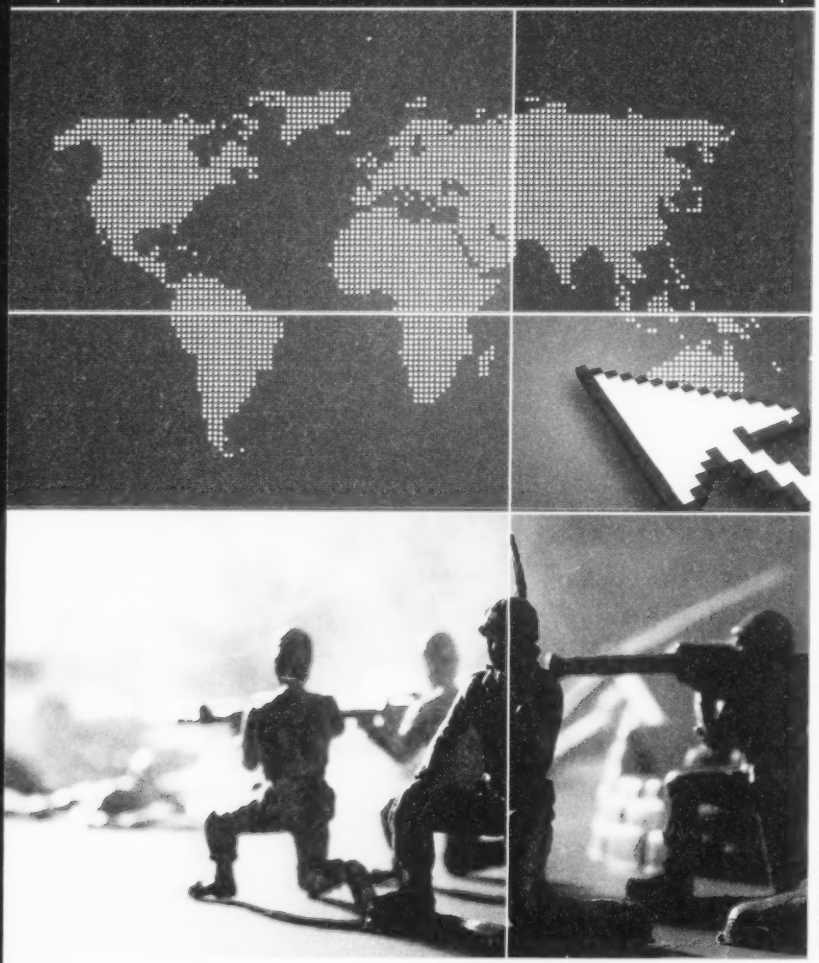
www.computerworld.com

COMPUTERWORLD

SPECIAL REPORT

The Fog of (CYBER) War

Cybermilitias, black hat hackers and other non-nation-state bad guys blur the lines on the virtual battlefield. By Don Tennant



ANALYSTS AND STRATEGISTS gathered at the Cyber Warfare 2009 conference in London last January were grappling with some thorny problems associated with the threat of Internet aggression. One that proved particularly vexing was the question of exactly what constitutes cyberwarfare under international law. There's no global agreement on the definitions of cyberwarfare or cyberterrorism, so how does a nation conform to the rule of law if it's compelled to respond to a cyberattack?

Back in the U.S. trenches, drawing up a legal battle plan is indeed proving to be extraordinarily complex. Those definitions are especially elusive when you consider that, in the foggy realm of cyberwarfare, no one can even be sure who the potential combatants are.

"There is some real work that needs to be done, not only in the U.S., but globally, to think about what is a use of force or an act of war in cyberspace," says Paul Kurtz, a partner at Good Harbor Consulting LLC in Arlington, Va., and a former senior director for critical infrastructure protection on the White House's Homeland Security Council.

The need to establish global norms about what is acceptable behavior in cyberspace, he says, is complicated by the fact that "the weapons are not just in the hands of nation-states. They're essentially in everybody's hands."

"Laws of war would forbid targeting purely civilian infrastructure," adds Steven Chabinsky, senior cyber adviser to the director of national intelligence. "But terrorists, of course, don't limit themselves by the Geneva Conventions."

TIME, EFFORT AND EXPERTISE

Further obscuring the battlefield is the fact that it's nearly impossible to identify all of the potential targets. However, it is possible to conduct a threat assessment, and there appears to be consensus in the cyberdefense community that nation-states pose the biggest threat.

"Cyberattacks which seek to manipulate [an adversary's] critical infrastructures would take more time, effort and expertise than mere data theft," says Kenneth Geers, U.S. representative to the Cooperative Cyber Defence Centre of Excellence in Tal-

Continued on page 30

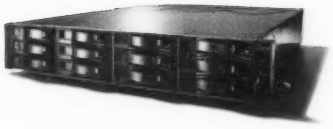
HIGHER PERFORMANCE SHOULDN'T WASTE YOUR ENERGY.

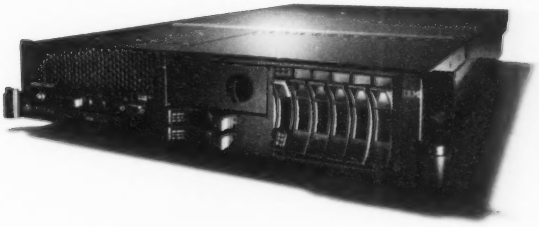
Get the high-performance servers your company needs without having to worry about rising energy costs. Introducing the IBM® System x3650™ M2 Express, with blazing fast, ultra-energy-efficient Intel® Xeon® 5500 processors and the IBM Systems Director Active Energy Manager,™ designed to monitor energy consumption, so you can better plan your energy usage and manage operating costs.

IBM express advantage™

BUNDLE AND SAVE
Act now. Available through IBM Business Partners.

ibm.com/systems/knowyourenergy
1 866-872-3902 (mention 6N8AH16A)





IBM SYSTEM STORAGE™ DS3200™ EXPRESS

$4,495.00

OR $119/MONTH FOR 36 MONTHS[1]

PN: 172621X

External disk storage with 3 Gbps serial attached SCSI (SAS) interface

Easy to deploy and manage with the DS3000 Storage Manager

IBM SYSTEM x3650™ M2 EXPRESS

$2,029.00

OR $54/MONTH FOR 36 MONTHS[1]

PN: 7947E1U

Featuring up to 2 Intel Xeon 5500 processors with speeds up to 2.93 GHz/6.4 GT

Energy-efficient design incorporating low 675 W and 92% efficient PS, 6 cooling fans, altimeter

Up to 128 GB via 16 DIMM slots (availability 2Q 2009) of DDR3 memory with clock frequency up to 1333 MHz

[1] IBM Global Financing offerings are provided through IBM Credit LLC in the United States and other IBM subsidiaries and divisions worldwide to qualified commercial and government customers. Monthly payments provided are for planning purposes only and may vary based on your credit and other factors. Lease offer provided is based on an FMV lease of 36 monthly payments. Other restrictions may apply. Rates and offerings are subject to change, extension or withdrawal without notice. IBM hardware products are manufactured from new parts or new and serviceable used parts. Regardless, our warranty terms apply. For a copy of applicable product warranties, visit www.ibm.com/servers/support/machine_warranties. IBM makes no representation or warranty regarding third-party products or services. IBM, the IBM logo, IBM Express Advantage, System Storage and System x are registered trademarks or trademarks of International Business Machines Corporation in the United States and/or other countries. For a complete list of IBM trademarks, see www.ibm.com/legal/copytrade.shtml. Intel, the Intel logo, Xeon and Xeon Inside are trademarks of Intel Corporation in the U.S. and other countries. All other products may be trademarks or registered trademarks of their respective companies. All prices and savings estimates are subject to change without notice, may vary according to configuration, are based upon IBM's estimated retail selling prices as of 3/4/09 and may not include storage, hard drive, operating system or other features. Reseller prices and savings to end users may vary. Products are subject to availability. This document was developed for offerings in the United States. ©2009 IBM Corporation. All rights reserved.

CYBERWEAPONS

According to former National Reconnaissance Office official Mike Theis, terrorists and criminals pose similar threats when it comes to making money illegally. Here are some activities these groups might undertake:

- Theft of personal information that could be sold to the highest bidder or on an information exchange.
- Theft of trade secrets, intellectual property or superior business processes. "It could be something as simple as your customer list, but there is usually a lot more of value than that," Theis says.
- Cyber-hostage-taking. If the contents of your entire hard drive were remotely encrypted by a hacker, would you pay $100 to get the decryption key? Would 10,000 people like you do the same?
- Cyberblackmailing. How much would you pay to prevent your family, customers, competitors or regulators from knowing something that was found on your computer?
- Cyberslaving. The perpetrator installs a back door or "loader" on your machine and sells it to the highest bidder. It would allow the buyer to install any type of software on that machine without being detected. "The last I heard, the average price was still about $1 per machine," Theis says. "It's not uncommon to see machines purchased in blocks of 10,000 or more in order to launch a denial-of-service attack."

"So basically," Theis says, "anything that can be done in the world of brick and mortar has some type of a cyber equivalent."

– DON TENNANT

Continued from page 28

linn, Estonia. "But computer network defenders should understand that time, effort and expertise are resources that militaries and foreign intelligence services often have in abundance."

Analysts and former intelligence officials, including Kurtz, say that, not surprisingly, China and Russia top the list of countries with highly developed cyberwarfare capabilities. Kurtz also points to Iran and North Korea as countries with known cyberwarfare aspirations.

While Chabinsky declines to be specific because of concerns about compromising intelligence-gathering methods, he affirms that the U.S. has identified "a number of sophisticated nation-state actors who we believe have the capability to bring down portions of our critical infrastructure." Fortunately, he adds, "we don't think they have the intent to do so, [since] our country would respond accordingly, and not necessarily symmetrically, through cyber means."

On the other hand, Kurtz notes, governments "would have more resources at their disposal in order to disguise or bury the true source of an attack." But, he says, "it would be a grave mistake to believe that a small, well-funded cell could not inflict very serious damage on the information infrastructure supporting the U.S. and the global economy."

Chabinsky notes that national governments are more comfortable grappling with the challenge of deterring or responding to cyberthreats from other countries. "There's a lot more to worry about should the same computer network attack capabilities exist in the hands of irrational or otherwise unrestrained criminals or terrorists," he says.

Intelligence officials and analysts agree that so far, there has been little direct threat of a cyberattack by organized terrorist groups. "Nonstate actors such as al-Qaeda probably do not possess the infrastructure or expertise to attempt a cyberattack that would rival the shock value of using bullets and explosives," Geers says.

But those officials and analysts recognize that terrorist groups have the resources and motives to fund such activities by others.

Although terrorists may not be capable of attacking our critical infrastructure themselves, "it's less clear whether they could find a hired gun to do so," Chabinsky says. "Obviously, terrorist groups have the intent to harm us, are aware of the potential impact of a successful cyberattack and would find the ability to attack us from a distance quite appealing."

"Insider threats can take advantage of the most serious vulnerabilities; in fact, they can create them.

STEVEN CHABINSKY, SENIOR CYBER ADVISER TO THE DIRECTOR OF NATIONAL INTELLIGENCE

According to Chabinsky, some potential "hired guns" are in an extraordinarily effective position to cause trouble: within the walls of corporate America.

"I think the primary cyber-risk to our critical infrastructure is from disgruntled employees who have insider knowledge and access," Chabinsky says. "Insider threats can take advantage of the most serious vulnerabilities; in fact, they can create them. Could they sell their capabilities to a terrorist group? Certainly."

CRIMINAL ELEMENT

To make matters worse, it's not only terrorist groups that are equipped to pose this sort of threat. In fact, they may not even be the most ominous nongovernmental source of potential cyberdamage.

"I would say that organized criminal activity provides a more pervasive and damaging threat than organized

terrorists," says Mike Theis, who until recently served as chief of cyber counterintelligence at the National Reconnaissance Office, an agency of the U.S. Department of Defense.

But that could change, Theis says.

While the motives of organized terrorists and organized criminals differ, their profit-generating tactics are mostly the same. Terrorists use cybercrime to fund their ideology-inspired activities, and criminals do it for the sake of profit itself (see "Cyberweapons," page 28).

Theis cites the infamous Russian Business Network as an example of the cybercriminals highest on the most-wanted list, but he pointed out that it would be difficult to name any organized crime syndicate that's not heavily engaged in electronic crime.

"Traditional organized crime has now moved to cyberspace to commit, support and enhance their crimes," says Ira Winkler, founder and president of Internet Security Advisors Group and a *Computerworld* columnist. These crime syndicates are "performing intelligence and counterintelligence collection of their own to see what governments are doing to stop their efforts."

Moreover, Winkler says, drug cartels, organized crime gangs and terrorist organizations are joining forces to combat the U.S. military and law enforcement agencies. "Possibly most important is that Russian crime gangs are heavily involved with the Taliban and al-Qaeda in the distribution of the poppy crops they grow," he says. "They are interested in stopping any coalition efforts to slow down the poppy distribution."

According to Chabinsky, cybercriminals have increased the scope and sophistication of their activities beyond those of all but a few nation-states. "There's big money to be had over the Internet, and organized crime is spending a lot of time and money to enhance their tradecraft," he says. "Organized cybercrime concerns me not just because of the money being stolen, but because cybercriminals are gaining the capacity to harm our critical infrastructure and could be motivated to do so as part of an extortion scheme."

Adding to the complexity of the problem are questions about the preparedness of other countries to combat the threat. "There is reason to consider whether some nation-states lack the ability to control organized crime within their borders, lack the resources to control criminals who victimize people and businesses outside their borders, or suffer from corruption in which government officials are complicit in lucrative criminal schemes," Chabinsky says.

THE HACKER MYTH

Another complicating factor is that these criminal elements are anything but cohesive units with consistent objectives.

"One of the things that's very tricky about cyberspace is you can have criminal organizations easily morph with hacker organizations, and you may have a cell within that that may have a different purpose or objective than the criminal organization," Kurtz explains. "This comes down to the essence of what makes the cyber tradecraft so complex. It's only a keystroke difference between getting inside someone's system and shutting it down."

Indeed, the role that hackers play in cyberwarfare is widely underestimated. "A big myth is that cybercrime is still about a 15-year-old kid doing Web defacements," Chabinsky says.

In truth, the hacker element is gaining influence and is being courted by governments. In China, hacker groups have traditionally been motivated by national pride, says Carl Setzer, an associate partner at Dallas-based iSight Partners, a security research firm that monitors hacking communities in China.

The Chinese government has channeled that pride toward its own ends, even though it may not issue direct orders to hacker groups. Setzer says that iSight has found evidence of direct interaction between Chinese hackers and the government — a relationship that he characterizes as "indirect control."

According to Winkler, China has to acknowledge the problem. "They have the Internet so filtered that even if [cybercrime] is not supported by the Chinese government, given the hold they have on their Internet connections, they can't claim clean hands," he says. "For them to say 'We aren't noticing attack traffic' is absurd."

Of course, the Chinese government is hardly alone in its goal of manipulating of hackers. Theis says cyberconflicts anywhere in the world that are

SAVE ENERGY WITHOUT WASTING YOUR OWN.

With IBM® System x3550™ M2 Express and the IBM Systems Director Active Energy Manager™

IBM express advantage™

ibm.com/systems/energysaver
1 866-872-3902 (mention 6N8AH17A)

IBM SYSTEM x3550™ M2 EXPRESS
$1,815.00

PN: 7946E1U

Featuring Intel® Xeon® 5500 processor with speeds up to 2.93 GHz/6.4 GT

Energy-efficient design incorporating low 675 W and 92% efficient PS, 6 cooling fans, altimeter

Up to 128 GB via 16 DIMM slots (availability 2Q 2009) of DDR3 memory with clock frequency of up to 1333 MHz

IBM hardware products are manufactured from new parts or new serviceable used parts. Regardless, our warranty terms apply. For a copy of applicable product warranties, visit www.ibm.com/servers/support/machine_warranties. IBM makes no representation or warranty regarding third-party products or services. IBM, the IBM logo, IBM Express Advantage, System Storage and System x are registered trademarks or trademarks of International Business Machines Corporation in the United States and/or other countries. For a complete list of IBM trademarks, see www.ibm.com/legal/copytrade.shtml. Intel, the Intel logo, Xeon and Xeon Inside are trademarks of Intel Corporation in the U.S. and other countries. All other products may be registered trademarks or trademarks of their respective companies. All prices and savings estimates are subject to change without notice, may vary according to configuration, are based upon IBM's estimated retail selling prices as of 3/4/09 and may not include storage, hard drive, operating system or other features. Reseller prices and savings to end users may vary. Products are subject to availability. This document was developed for offerings in the United States. © 2009 IBM Corporation. All rights reserved.

A SHORT HISTORY OF HACKS, WORMS AND CYBERTERROR

- 1964: AT&T cracks down on "phreakers," who use tone generators to make free phone calls.
- 1971: John Draper, later known as Captain Crunch, uses a whistle given away as a prize in a cereal box to gain access to AT&T's phone network.
- 1978: Engineers at Xerox Palo Alto Research Center design what they call a "worm" program to improve efficiency by searching for underused processors on a network.
- 1983: The FBI busts young hackers known as the 414s, who use an Apple II+ and a modem to break into 60 computer systems.
- 1986: "The Brain," one of the first PC viruses, is released in Pakistan.
- 1988: Grad student Robert Morris Jr. releases a worm that invades the Arpanet, disabling about 6,000 computers and clogging systems.
- 1994: Hackers led by Russian Vladimir Levin steal millions from Citibank.
- 1995: Hacker Kevin Mitnick is charged with wire fraud and possession of files stolen from companies such as Motorola and Sun Microsystems.
- 1996: Hackers alter the Web sites of the U.S. Department of Justice, the CIA and the Air Force.
- 1998: The Solar Sunrise attacks exploit vulnerabilities in Solaris to implant sniffer programs in more than 500 military, government and private-sector computer systems.
- 1999: The Melissa worm infects thousands of computers, causing an estimated $1.5 billion in damage.
- 2000: Russian hackers penetrate Microsoft. The ILOVEYOU worm infects millions of computers worldwide in a few hours. DDoS attacks knock Amazon, Yahoo and eBay offline.
- 2001: The Code Red worm, designed to use the combined power of a network of infected machines against the White House Web site at a predetermined date, is blocked as the attack begins.
- 2002: The Klez worm sends copies of itself to all of the e-mail addresses in its victims' directories.
- 2003: A Russian hacker group known as the Hang-Up Team builds a Web site featuring administrative tools for attacking U.S. financial institutions.
- 2004: The Secret Service arrests 28 people for exposing confidential Secret Service documents.
- 2006: Jeanson James Ancheta is imprisoned for attacks on the Naval Air Warfare Center and the Defense Information Systems Agency.
- 2007: Estonia suffers a massive DDoS attack that knocks out government and banking networks.
- 2008: Chinese hackers claim to have gained access to the world's most sensitive sites.
- 2009: The GhostNet infects computers in 103 countries, stealing documents and taking control of webcams. A hack thought to have originated in China steals data on the Pentagon's Joint Strike Fighter program.

– COMPILED BY MARI KEEFE

"I would say that currently, organized criminal activity provides a more pervasive and damaging threat than organized terrorists."

MIKE THEIS, FORMER CHIEF OF CYBER COUNTERINTELLIGENCE, NATIONAL RECONNAISSANCE OFFICE

attributed to "patriotic hackers" tend to be the stuff of myth. Usually, he says, they're the "well-thought-out efforts of nation-states with well-developed strategies and resources."

Although Theis has no doubt that patriotic hackers participate in cyberconflicts, he's convinced that far more is ascribed to them than real-world conditions would sensibly allow.

"To be truly effective on anything other than the smallest of scales takes strategic planning, resourcing and practiced execution to ensure activities are focused at the right place and time to be a force multiplier, and not wasted on the overkill of nonessential targets or activities," Theis says. "It seems ludicrous that countries that have stated their understanding of the importance of cyberconflict dominance and have dedicated resources to that effort would not use them in a decisive way but [instead] would depend on patriotic hackers to just happen to get it right and just at the right time."

Still, governments have every reason to foster the idea that patriotic hackers are at work, Theis says. "It's a nice myth to perpetuate if you're trying to maintain plausible deniability." ■

Jeremy Kirk *and* **Sumner Lemon** *of the IDG News Service contributed to this story.*

Attention to Conficker Appears to Pay Off

The **notorious worm** has the security team putting **all its focus** on **protecting** the company's **9,000 systems** around the globe.

Trouble Ticket

AT ISSUE: It appears possible that the Conficker worm could wreak more havoc than usual.

ACTION PLAN: Keep it out of the network to the extent possible, by focusing on updating antivirus software and Microsoft patches.

LIKE JUST about every other IT department, mine spent the week before April Fools' Day preparing for the onslaught of the Conficker worm.

This bit of malware got a lot of attention in the press, and I decided that it would be best to do everything possible to alleviate its effects, even if that meant overreacting. After all, there was no way to know for sure just what could transpire if our systems were infected with the worm come April 1, the date Conficker was scheduled to "receive new commands" from whoever had devised it and sent it into the world.

During the last week of March, I started arranging meetings and gathering data. I decided to focus our efforts on virus signatures and patch management. I figured that if we made sure every machine in our current inventory was up to date with the latest antivirus pattern file and Microsoft security patches, then we would have a good shot at being protected against any Conficker variant.

In analyzing our patch status, I was especially interested in Microsoft Security Bulletin MS08-067, for a vulnerability in the Windows Server service that could allow the Conficker worm to propagate. I had our Windows Server team run a Microsoft Systems Center Configuration Manager report to find out whether all our servers and desktops had the proper patch.

I also contacted Trend Micro, our vendor for desktop and server virus protection, to ensure that it would have the proper signatures to detect Conficker. Trend Micro responded that the then-current pattern file would be sufficient to protect us, so I found it interesting that we received two or three updated pattern files from Trend Micro in the last days of the month, all seeming to focus on Conficker variants.

■ On March 30, two days prior to Armageddon, we had a 98% compliance rate with antivirus and 95% for the Microsoft patch.

Finally, I had the team do a last-minute push to ensure the most comprehensive level of compliance.

COUNTDOWN

On March 30, two days prior to Armageddon, we had a 98% compliance rate with antivirus and a 95% compliance rate for the Microsoft patch. We have over 9,000 devices running a Windows operating system, so 2% and 5% noncompliance could be big problems, but I was fairly content.

I've never been able to achieve 100% compliance for a variety of reasons: Some engineering computers can't be patched, a segment of our workforce is highly mobile and doesn't connect to the network on a regular basis, and we have a global footprint and therefore encounter many problems related to time zones.

For additional protection, I had my security engineers scour the Internet for intrusion-detection signatures for activity associated with Conficker. We use both Snort and Juniper for intrusion detection and were fortunate to find plenty of Snort signatures, and Juniper provided additional signature files.

More unusual for such an event, we had to manage communications. This worm had made headlines, prompting calls to the help desk and queries from executives. I drafted an e-mail message assuring everyone that we were on top of the Conficker situation. While I was at it, I reminded all employees to practice safe computing and not open attachments from untrusted sources or visit unvalidated URLs.

April 1 came and went. Our intrusion sensors detected a few systems in China that were generating unusual amounts of traffic. We were able to track down those machines quickly, isolate them and eliminate the problems.

Of course, not one of those machines had been patched or was running properly updated antivirus software. ■

This week's journal is written by a real security manager, ***"Mathias Thurman,"*** *whose name and employer have been disguised for obvious reasons. Contact him at mathias_thurman@yahoo.com.*

COMPUTERWORLD.COM

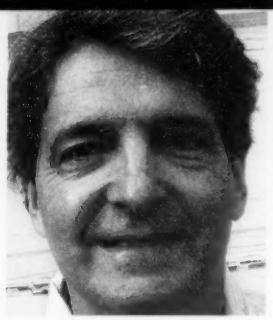
JOIN IN

To join in the discussions about security, go to **computerworld.com/blogs/security**

■ OPINION

Preston Gralla

Cyberwarfare's First Casualty



THE FIRST CASUALTY OF WAR, the Greek playwright Aeschylus said, is the truth. But when it comes to cyberwarfare, the first casualty will most likely be your privacy.

And unlike in past wars, the government itself may not do the snooping. Instead, it will most likely let private industry do the dirty work, essentially outsourcing cyber-intelligence-gathering.

In warfare, information is one of the most important weapons in a government's arsenal. No matter the physical weaponry, the key to victory is an understanding of the enemy's intentions and who and where he is. Analyze any war, and you'll generally find that the victor had better intelligence.

As we've seen, though, intelligence-gathering is frequently subject to abuse. During the Cold War, the CIA and FBI regularly violated the rights of U.S. citizens. More recently, the Patriot Act gave legal cover to government prying, and the National Security Agency carried out covert wiretapping without seeking the proper warrants.

The intelligence that will be gathered in the coming generation of cyberwarfare will dwarf anything that came before, in the breadth of information acquired, the ease with which it is gathered, and the number of people caught in the net. In past wars, a fair number of innocent people had their privacy invaded. In tomorrow's cyberwar, it'll be virtually everyone.

Cyberwarfare is fought online; its geography is virtual, and you're part of it. In physical wars, armies scout the countryside. In cyberwars, they'll scout the Internet.

The Internet is made up not just of wires, routers and servers; it's made up of the data crossing it. Those who fight cyberwars will mine vast amounts of data in an attempt to find nuggets of information. They'll look for patterns of use and relationships that would otherwise escape notice.

■ In past wars, a number of people had their privacy invaded. In cyberwars, it'll be virtually everyone.

To find those patterns and information requires massive and constant data-gathering, on a scale likely not being done by the government. Constantly gathering that kind of information would probably be illegal.

That's why you'll see government outsourcing its intelligence-gathering to companies that already do the work legally — and primarily that means Google.

I'm not saying that Google will purposefully gather information for the federal government. Instead, the government will legally tap into Google's already-in-place information-gathering by issuing subpoenas on a regular basis.

Why Google? Google already gathers vast amounts of information about people's browsing and search habits, and it regularly responds to subpoenas for that data.

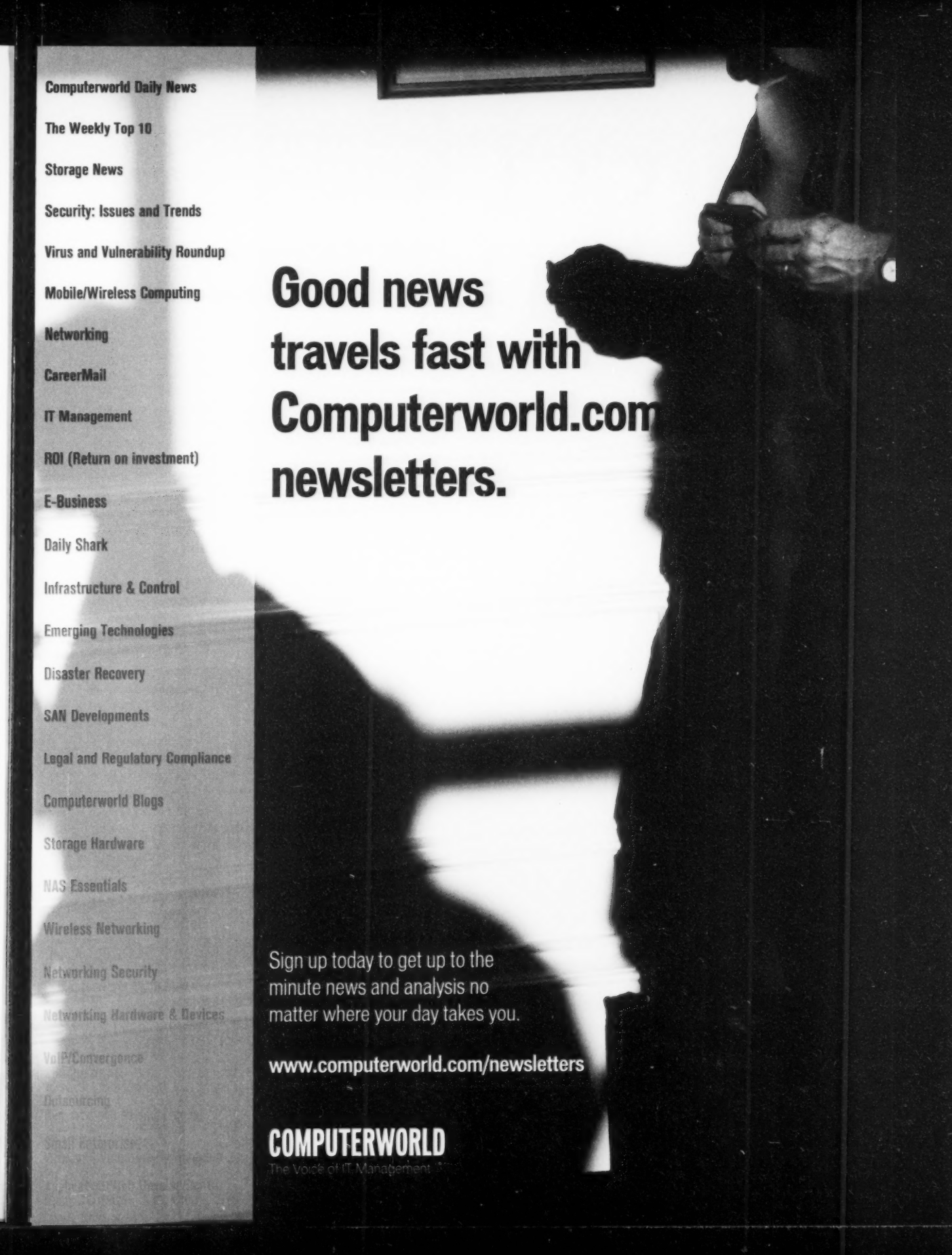
And the information that Google gathers is about to grow exponentially, when Google Voice expands to widespread use. Google Voice will route all of your calls through a single number, let you record and store calls online, and offer transcripts of voice mail. At some point, it will probably offer transcripts of all calls recorded. It will be able to do that for your normal voice calls, not just calls made to or from a computer.

You can be sure that the government will want to get its hands on that vast treasure trove of information. Just think about it: Why go through the difficult process of getting a phone tap when it's so much easier to simply issue a subpoena to Google?

Google isn't alone, of course; many other private companies — particularly ISPs and big telecom providers — also gather information about people online. But no one gathers the amount of information about people that Google does. So it will become the government's biggest source of information about private citizens in the age of cyberwars.

The upshot? If you care about your privacy, your best bet is to find ways to hide your information from Google. Private companies, more than the government, will be the biggest privacy invaders. ■

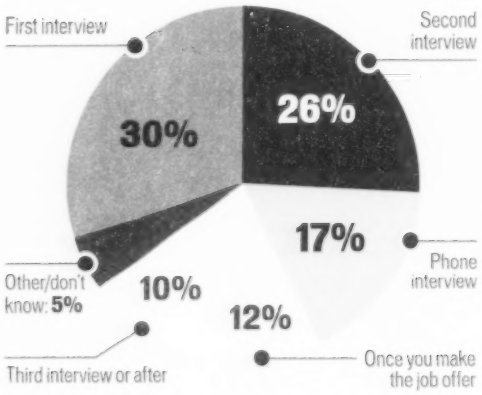
Preston Gralla *is a contributing editor for* Computerworld.com *and the author of more than 35 books, including* How the Internet Works *(Que, 2006).*


Computerworld Daily News
The Weekly Top 10
Storage News
Security: Issues and Trends
Virus and Vulnerability Roundup
Mobile/Wireless Computing
Networking
CareerMail
IT Management
ROI (Return on investment)
E-Business
Daily Shark
Infrastructure & Control
Emerging Technologies
Disaster Recovery
SAN Developments
Legal and Regulatory Compliance
Computerworld Blogs
Storage Hardware
NAS Essentials
Wireless Networking
Networking Security
Networking Hardware & Devices
VoIP/Convergence
Outsourcing
Good news travels fast with Computerworld.com newsletters.
Sign up today to get up to the minute news and analysis no matter where your day takes you.
www.computerworld.com/newsletters
COMPUTERWORLD
The Voice of IT Management

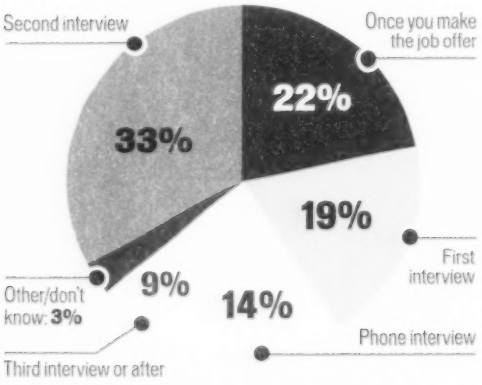
Career Watch

Getting to the Bottom Line

Senior executives were asked, "When is it appropriate for job candidates to ask about compensation and benefits during the hiring process?" Their responses:



The executives were also asked, "When is it most common for you to discuss compensation and benefits with a potential hire?" Their responses:



SOURCE: ACCOUNTEMPS TELEPHONE SURVEY OF 150 SENIOR EXECUTIVES AT LARGE COMPANIES, FIRST QUARTER 2009

PAGE COMPILED BY JAMIE ECKLE

ASK A PREMIER 100 IT LEADER

Mark Burnette

An expert in leadership, IT process, compliance, security and cost management who has led two award-winning IT organizations, Burnette answers questions about surviving the economic downturn and returning to school.

My company hasn't laid off anyone from IT yet in this stagnant economy, but I'm sure it's just a matter of time. Any advice on how to avoid the ax when it comes down? First, don't run around afraid you're going to lose your job. It will affect your mind-set, which in turn will subconsciously affect how you perform and how you interact with your co-workers. Plus, it's no fun to go to work in a negative state of mind all the time. Second, focus on results. No matter how much you're paid, if you consistently meet or exceed your boss's expectations, it will be very difficult for him to put your name on the pink slip when decision time comes.

If you're not sure of your status in your boss's eyes, seek constructive feedback and act immediately on any improvement suggestions. Be reliable, and communicate consistently and effectively with your co-workers. And last, being a trusted subject-matter expert on a particularly important technology solution for your company will make it difficult to cut you loose as well. But don't fall into the trap of trying to "hoard" information so that you'll be the only expert in that area. Your boss will notice and may assume you're not a team player.

While doing all of this, you should also get your ducks in a row in case you do lose your job. Update your résumé (after-hours) to reflect all of your current experience; gather any performance reviews, job descriptions, etc., that may be helpful if you have to look for another job. Many employers are using LinkedIn as a reference tool when considering prospective employees, so update your LinkedIn profile, and consider asking some co-workers to "endorse" you there. Build your professional network by attending trade association or professional organization events and meeting people. In the business world, landing that next job is often more about *who* you know rather than simply *what* you know.

COMPUTERWORLD.COM

QUESTION?

If you have a question for one of our Premier 100 IT Leaders, send it to **askaleader@computerworld.com**, and watch for this column each month.

I've been toying with the idea of going back to school. (I work in desktop support and want to learn more about networking and business matters.) I'm thinking that this economy is a good time to do it. What areas should I focus on that would give me a leg up when the economy turns around? Information security is a great field of study because all organizations are dealing with security issues on some level. Even companies that aren't focusing on building a security function – and most of them are, given the visibility and liability of security breaches – have to deal with compliance issues of some type, and achieving compliance typically involves layering in control processes or technology that requires some degree of security knowledge. Further, technical security work, such as vulnerability assessment, intrusion detection and forensics, requires a specialized skill set that commands a compensation premium at most companies.

Burnette can be reached at mark@markburnette.com.

COMPUTERWORLD

100

BEST PLACES

TO WORK IN IT 2009

Take this opportunity to show why your company is an employer of choice to the IT community!

Over 1,000,000 qualified IT professionals will be looking to this must-read issue for future career opportunities. Don't miss out on Computerworld's biggest and most anticipated career issue of the year!

Issue Date: June 15th
Space Deadline: June 1st

For details contact:
Dawn Cora at 508-820-8133
dawn_cora@idgcommunications.com

Trinity Consulting seeks system analysts, s/w engineers, DBA, IT Managers to customize applications per using Java, J2EE, .NET, Cognos, SAP, Oracle etc. Require MS or BS w/ exp. Travel required. Please contact bikki@trinity-world.com. EOE

IT Professionals (program/ system analyst, software engineer, DBA) wanted by Thinc Systems to handle IT projects using VB, Oracle, Java, J2EE, Weblogic, Websphere, SAP, etc. Require MS or BS w/ exp. Travel required. Please contact bikki@thincsys.com. EOE

Labor Certification Ads

Are you an individual, agency or law office needing to place ads to fulfill legal requirements?

Let us help you put together an efficient, cost-effective program that will help you place your ads quickly and easily.

For more details, contact us at:
800.762.2977
IT|careers

Didn't find the IT career that you were looking for?

Check back with us weekly for fresh listings placed by top companies looking for skilled professionals like you!

IT|careers

IT Professionals - Broadridge Financial Solutions is looking for senior technical directors and technical consultants (Jersey City, NJ), director of production (Peabody, MA), senior and lead programmer analysts (Hingham, MA, San Francisco, CA, Wheat Ridge, CO, and New York City, NY) and senior business analysts (New York City, NY), senior database administrator (Wheat Ridge, CO) and for quality assurance analysts (Jersey City, NJ). Offered positions require a master's and bachelor's degree and/ or work experience in the position or in alternative occupation, any suitable combination of education, training and work experience. Resumes to Broadridge HR by fax to 212-591-6623 or e-mail HiringInfo@aol.com EOE

Eldorado Computing Inc has multiple openings for the following professional positions at its office in Phoenix, AZ office.

1. Technical Analyst – Review system and develop migration tools. 2. Systems Specialist – Analyze sys w/solution to improve its capabilities.

Must have Bachelor or Master or equivalent & prior exp in job offered or related field. Edu/exp reqs vary depending on position level/type. May require travel/relocation. Please send resume, salary history and position applied for to recruitment@mhs.mphasis.com or 5353 N 16th, Suite 400, Phoenix, AZ 85016 Attn: HR. w/ Ref.CW0409

Sr. Software Developer - Engage in full life-cycle s/ware dvlpmt of internet & client/ server GIS mapping applics in a team envrmt. Req's incl. Master's in Comp Sci or rel. field or eqv. & working knowl of dvlpg & maintaining web & Windows-based GIS mapping applics, SQL/Server, & Active Directory. Resume to: IntraSearch, Pat Salling, 5340 South Quebec St., 300S, Greenwood Village, CO 80111.

Software Engineer, Systems. Woodstock GA. Dvlp mkt integration algorithms for automated demand response/ real-time price energy cntrl programs. Bach's + 1 yr exp or 1 yr exp as Sr Web Dvlpr. Send resume to: Linda Johnston, RTP Controls Inc. 250 Churchill Ct, Unit 100, Woodstock GA 30188

Apollo Group located in Phoenix, AZ has multiple openings for IT professionals. Specific skill sets needed include:

- .Net developers JO-010
- JAVA/J2EE JO-020
- Data warehousing developers JO-030
- Oracle Developers/DBA JO-040
- Quality Assurance Analysts JO-050
- Systems Administrators JO-060
- Web-based Developers JO-070
- Business Analysts JO-080
- PeopleSoft JO-090

All positions require at least a B.S. degree in related field. Some positions require an M.S. degree. Competitive salaries. Send resume to: pat.branum@phoenix.edu. Refer to specific JO# for consideration. Applicants must have authority to work permanently in the U.S.

Innowave Technology, LLC is seeking a Software Consultant in Oracle Technology for office in Irvine, CA. B.Sc. or equivalent in engineering or related field and 3 years of work exp. in oracle technology products. Salaried/full time position. For details about this & other job opportunities, please visit www.innowavetech.com. Please mail CV & salary requirements to 2151 Michelson Drive #230, Irvine, CA 92612 or fax to 949-223-6428

Computer Professionals for NJ based IT firm: Sr. Level: IT Manager, MIS Manager, ITS Director, Project Manager needed to plan, direct, coordinate activities in such fields as electronic data processing, information systems, systems analysis & computer programming. Jr. Level: Programmer Analysts, Software Engineers, Systems Analyst to Develop, create & modify general computer applications software or specialized utility programs. Analyze user needs and develop software solutions. Apply w/2 copies of resume to JSMN International, Inc.591Summit Ave, Suite # 522 Jersey City NJ 07306

Sr & Jr Software Engineers. Multiple positions in NO VA & other sites. Design & develop Data Warehousing & other applns using client server technology. May Req Travel. BS or MS in CS, Engg(any) or rel w/ 2-5 yrs exp. Skills such as Ab Initio, HP Unix/Linux, Oracle/ Teradata. Send resumes to Avaron, Inc. 2325 Dulles Corner Blvd, #500, Herndon,VA 20171.EOE.

Shark Tank

TRUE TALES OF IT LIFE AS TOLD TO SHARKY

A Little Too Smart For Its Own Good

It's the 1990s, and this IT pilot fish works for a wholesale distributor. "We shut down on Sundays but otherwise ran pretty much 24 hours a day," fish says. "We came in one Monday morning and found the computer room baking the equipment at 100-plus degrees. The air conditioning unit had died. Some equipment was smart enough to power down. Other equipment fried. We didn't understand why no automatic call had gone out to us about the problem. After a bit of checking, we found that the new phone switch was smart enough to take itself down when the temperature got too warm. Unfortunately, it did so *before* the emergency sensor was triggered and tried to call us. Within a week, we had a dedicated phone line that didn't go through the 'smart' switch."

That Would Explain It

This pilot fish is pretty new to the help desk when he gets a call from a user who can't connect to the corporate VPN from home. "He was using one of our laptops, so I went through the usual troubleshooting steps and determined that it was the Internet connection," says fish. "He swore that his other computers could access the Internet fine and that it must just be the crappy work laptop. I finally got him to check one of his home PCs and, lo and behold, no Internet access. He was getting an IP address from his router, and the wireless signal was good, so I suggested checking the cable modem. He stepped away, then came back a few minutes later to say, 'The cable modem is out, and the TV is all fuzzy. And I saw my wife out back with the hedge clippers.' Maybe our laptops aren't that bad after all."

Thanks, Kiddo

Consultant pilot fish gets – "on rare occasions," he says – good reviews from his clients. "This one client must have been so utterly impressed that he told his daughter about how I quickly and correctly solved one of his problems," says fish. "And since they were at the same university, his daughter told my daughter. To which my daughter commented: 'Are you sure he's talking about my father?' "

This week marks exactly 10 years since Sharky started retelling your true tales of IT life. Hard to believe anybody could spend that much time hanging around a water cooler. Sharky wants to thank his friends who have helped over the years: Steve, Frank, Sami, Mitch, Paul, Tom, Maryfran, Sharon, Linda, Jamie, Michele and the gang down at Bob's Poolroom. Special thanks goes to all the stalwart pilot fish who have told me their stories but must remain nameless — so they can remain employed. Want to join them? Send your tale to sharky@computerworld.com. I'll file off the identifying marks, and you'll score a sharp Shark shirt if I use it.

COMPUTERWORLD.COM

TIRED OF BUNGLING BOSSES and clueless co-workers? Swim on over to Shark Bait and share your tales of woe. **sharkbait.computerworld.com**

CHECK OUT Sharky's blog, browse the Sharkives and sign up for Shark Tank home delivery at **computerworld.com/sharky.**

COMPANIES IN THIS ISSUE

Page number refers to page on which story begins. Company names can also be searched at computerworld.com

Accutemps 36
Actuality Medical Inc. 15
Advanced Micro Devices Inc. 7
Alfresco Software Inc. 12
Amazon.com Inc. 32
Ascend Communications Inc. 16
Association for Competitive Technology 8
AT&T Inc. 32
BAE Systems PLC 4
Broadcom Corp. 7
Burton Group Inc. 14
Center for Strategic and International Studies 6, 22
CIA 32, 34
Cisco Systems Inc. 14
Citibank 32
Citrix Systems Inc. 14
CLR Choice Inc. 10
Cooperative Cyber Defence Centre of Excellence 28
Core Security Technologies Inc. 6
Craigslist Inc. 12
CSX Corp. 26
Defense Information Systems Agency 32
Dell Inc. 12
Digg Inc. 12
eBay Inc. 32
Embarq Corp. 10
EMC Corp. 7
Emulex Corp. 7
Fair Isaac Corp. 14
FBI 32, 34
Forrester Research Inc. 22
Fujitsu Ltd. 12
Good Harbor Consulting LLC 24, 28
Google Inc. 12, 34
Hewlett-Packard Co. 12, 18, 40
Homeland Security Council 4, 28
IBM 12
Idaho National Laboratory 24
IDC 12
Ingres Corp. 12
Insight64 7
Intel Corp. 7
Internet Corporation for Assigned Names and Numbers 24
Internet Security Advisors Group 31
iSight Partners 31
Juniper Networks Inc. 33
LinkedIn Corp. 36
Lockheed Martin Corp. 4
Los Alamos National Laboratory 32
Microsoft Corp. 6, 7, 8, 12, 14, 18, 26, 32, 33
Minnesota Supercomputing Institute 8
Motorola Inc. 32
National Aeronautics and Space Administration 7
National Communications System 24
National Cyber Security Center 22
National Reconnaissance Office 30, 31
National Security Agency 6, 22, 34
Naval Air Warfare Center 32
New York University 7
Northrop Grumman Corp. 4
Nucor Steel Tuscaloosa Inc. 12
Nvidia Corp. 16
Oracle Corp. 6, 10, 12, 40
Pan-European ICT and eBusiness Network for SMEs 8
Rackable Systems Inc. 8
RSA Security Inc. 6
Sandia National Laboratories 26
Sanford C. Bernstein & Co. 12
SANS Institute 26
SAP AG 6
Silicon Graphics Inc. 8
Software AG 12
Sony Ericsson Mobile Communications AB 8
Spectra Logic Corp. 7
St. Luke's Episcopal Health System 12
Sun Microsystems Inc. 6, 7, 8, 10, 12, 32, 40
Tata Consultancy Services Ltd. 8
Texas Instruments Inc. 16
The SecDev Group 21
Trend Micro Inc. 33
U.S. Air Force 32
U.S. Department of Defense 4, 8, 31
U.S. Department of Homeland Security 6, 21, 22
U.S. Department of Justice 32
U.S. Government Accountability Office 22
Unisys Corp. 26
University of Pennsylvania 7
University of Toronto 21
VMware Inc. 8, 14
Xerox Palo Alto Research Center 32
Yahoo Inc. 12, 32
YouTube Inc. 12

ADVERTISERS' INDEX

Accenture C2-1
accenture.com/outsourcing
CA 9
ca.com/apm
CA 23
ca.com/security
CA C3
ca.com/spectrum
Fujitsu Computer Systems Corporation 11
www.fujitsudailyfuel.com
Hewlett-Packard C4
hp.com/servers/virtual9
IBM Express Seller 29
ibm.com/systems/knowyourenergy
IBM Express Seller 31
ibm.com/systems/energysaver
Microsoft 17
SQLServerEnergy.com
Novell 3
moreinterop.com
Novell 13
novell.com/evolution
Storage Networking World 19
www.snwusa.com

This index is provided as an additional service. The publisher does not assume any liability for errors or omissions.

Periodical postage paid at Framingham, Mass., and other mailing offices. Posted under Canadian International Publication agreement PM40063731. **CANADIAN POSTMASTER:** Please return undeliverable copy to PO Box 1632, Windsor, Ontario N9A 7C9. Computerworld (ISSN 0010-4841) is published weekly, except for combined issues in November and the last week and first week of each of the following months: December/January, March/April, May/June, June/July, and August/September by Computerworld, Inc., 1 Speen Street, Box 9171, Framingham, Mass. 01701-9171. Copyright 2009 by Computerworld Inc. All rights reserved. Computerworld can be purchased on microfilm and microfiche through University Microfilms Inc., 300 N. Zeeb Road, Ann Arbor, Mich. 48106. Computerworld is indexed. Back issues, if available, may be purchased from the circulation department. Photocopy rights: permission to photocopy for internal or personal use is granted by Computerworld Inc. for libraries and other users registered with the Copyright Clearance Center (CCC), provided that the base fee of $3 per copy of the article, plus 50 cents per page, is paid directly to Copyright Clearance Center, 27 Congress St., Salem, Mass. 01970. Reprints (minimum 100 copies) and permission to reprint may be purchased from Ray Trybovich, ComputerworldReprints, c/o The YGS Group, Greenfield Corporate Center, 1808 Colonial Village Lane, Lancaster, Pa., 17601, (800) 290-5460, Ext. 148, Fax: (717) 399-8900, Web site: www.reprintbuyer.com, E-mail: computerworld@theygsgroup.com. Requests for missing issues will be honored only if received within 60 days of issue date. Subscription rates: $5 per copy; U.S. – $99.99 per year; Canada – $130 per year; Central & So. America: $250 per year; Europe – $295 per year; all other countries – $295 per year. Subscriptions: call toll-free (888) 559-7307. **POSTMASTER:** Send Form 3579 (Change of Address) to Computerworld, PO Box 3500, Northbrook, Ill. 60065-3500.

BPA WORLDWIDE ABM

COMPUTERWORLD

HEADQUARTERS
P.O. Box 9171, 1 Speen Street
Framingham, MA 01701-9171
(508) 879-0700
Fax (508) 875-4394

President/CEO
Matthew J. Sweeney
(508) 271-7100

Executive Assistant to the President/CEO
Diana Cooper
(508) 820-8522

Vice President/Group Publisher Program Sales
John Amato
(508) 820-8279

Vice President/ General Manager Online
Martha Connors
(508) 620-7700

Vice President, Marketing
Matt Duffy
(508) 820-8145

Editor in Chief
Scot Finnie
(508) 628-4868

Vice President, Custom Content
Bill Laberis
(508) 820-8669

Vice President, Human Resources
Julie Lynch
(508) 820-8162

Executive Vice President, Strategic Programs
Ronald L. Milton
(508) 820-8661

Vice President/Group Publisher Computerworld.com
Gregg Pinsky
(508) 271-8013

Executive Vice President/COO
Matthew C. Smith
(508) 820-8102

IDG

International Data Group Chairman of the Board
Patrick J. McGovern

CEO, IDG Communications
Bob Carrigan

Computerworld is a business unit of IDG, the world's leading technology media, research and events company. IDG publishes more than 300 magazines and newspapers and offers online users the largest network of technology-specific sites around the world through IDG.net (*www.idg.net*), which comprises more than 330 targeted Web sites in 80 countries. IDG is also a leading producer of 168 computer-related events worldwide, and IDG's research company, IDC, provides global market intelligence and advice through 51 offices in 43 countries. Company information is available at *www.idg.com*.

Sales Offices

NORTHWESTERN STATES
BAY AREA
Program Sales Director
Sandra Gibson (415) 978-3306
Senior Program Sales Associate
Chris Da Rosa (415) 978-3304
Mailing Address
501 Second Street, Suite 114
San Francisco, CA 94107
Fax (415) 543-8010

SOUTHWESTERN STATES
CENTRAL STATES
Program Sales Director
Lauren Guerra (415) 978-3306
Senior Program Sales Associate
Emmie Hung (760) 597-1386
Mailing Address
501 Second Street, Suite 114
San Francisco, CA 94107
Fax (415) 543-8010

SOUTHEASTERN STATES
Program Sales Director
Lisa Ladle-Wallace (904) 284-4972
Mailing Address
5242 River Park Villas Drive
St. Augustine, FL 32092
Fax (800) 779-8622
Senior Program Sales Associate
Jess Roman (508) 271-7108
Mailing Address
P.O. Box 9171, 1 Speen Street
Framingham, MA 01701
Fax (508) 270-3882

NEW ENGLAND STATES
Program Sales Director
Deborah Crimmings (508) 271-7110
Senior Program Sales Associate
Jess Roman (508) 271-7108
Mailing Address
P.O. Box 9171, 1 Speen Street
Framingham, MA 01701
Fax (508) 270-3882

METRO NEW YORK
EASTERN STATES
Program Sales Director
Hal Mentlik (631) 696-4498
Senior Program Sales Associate
John Radzniak (201) 634-2323
Mailing Address
650 From Road, Suite 225
Paramus, NJ 07652
Fax (201) 634-9289

Senior Sales Operations Manager
Dawn Cora (508) 820-8133

Director of Market Intelligence
Paul Calento (415) 978-3212
Mailing Address
501 Second Street, Suite 114
San Francisco, CA 94107
Fax (415) 543-8010

CIRCULATION/DISTRIBUTION
Vice President
Debbie Winders (508) 820-8193
Circulation Manager
Diana Turco (508) 820-8167
Distribution and Postal Affairs
Michelle Fuller (508) 628-4757

PRODUCTION
Vice President, Production
Carolyn Medeiros
Production Manager
Kim Pennett
Print Display Advertising
(508) 820-8232
Fax (508) 879-0446

STRATEGIC PROGRAMS AND EVENTS
Vice President, Business Development John Vulopas
(508) 271-8024
Vice President, Strategic Programs & Events Ann Harris
(508) 820-8667
Vice President, Event Marketing and Conference Programs Derek Hulitzky
(508) 620-7705
Senior Director, Event Management Michael Meleedy
(508) 820-8529
Senior Director, Executive Programs Sandy Weill
(508) 620-7758

ONLINE ADVERTISING
Vice President/Group Associate Publisher Sean Weglage (415) 978-3314
Fax (415) 543-8010
Online Sales Directors
James Kalbach
(610) 971-1588
Jennell Hicks
(415) 978-3309
Fax (415) 543-8010
Online Sales Managers
Matthew Wintringham
(508) 820-8218
Fax (508) 270-3882
Kristi Nelson
(415) 978-3313
Fax (415) 543-8010
Account Services Director
Bill Rigby (508) 820-8111
Fax (508) 270-3882
Online Sales Assistant
Joan Olson (508) 270-7112
Fax (508) 270-3882

IT CAREERS
Senior Sales Operations Manager
Dawn Cora (508) 820-8133
Fax (508) 626-8524

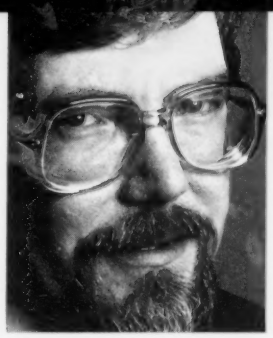
LIST RENTAL
Postal and E-mail
Rich Green (508) 370-0832
rgreen@idglist.com
Mailing Address
IDG List Services, P.O. Box 9151
Framingham, MA 01701-9151
Fax (508) 370-0020

Customer Service (888) 559-7327 toll free
Local or outside U.S. (847) 559-1573
E-mail: cw@omeda.com

■ FRANKLY SPEAKING

Frank Hayes

The 95% Question



LET'S FORGET ABOUT the software from that Oracle-Sun deal for a moment (see story, page 10). Yes, Oracle loves Java and Solaris — Oracle's middleware depends on Java, and lots of Oracle databases run on Solaris. And yes, Oracle will tolerate MySQL. OpenOffice, VirtualBox and other Sun software products? We'll see.

But all told, that's 5% of Sun's sales. What about the hardware?

If you're a Sun customer, that's probably what you're worried about. You've spent plenty on Sparc servers and maybe shelled out something for storage, tape systems and workstations. If it turns out that Oracle wants to remain a high-margin software company and quickly sells off the hardware lines, you'll suddenly have some expensive decisions to make.

Sure, Oracle says it "plans to grow the Sun hardware business . . . protecting Sun customers' investments and ensuring the long-term viability of Sun's products." That's from Oracle's official FAQ on the buyout.

But it's a little hard to believe. After all, Oracle is a software company that has just dabbled now and then in hardware. And these days, computing hardware is not an attractive business. Low margins. Slow growth. Brutal competition. Hardware is a commodity, and Oracle has worked hard to make it so.

Besides, why would Oracle want to keep — and invest in — a money-losing business that puts it in direct competition with HP, one of its most important partners?

I've got no inside information on that one. But I know this: Larry Ellison loves appliances.

Look, here's Ellison on the merger: "Oracle will be the only company that can engineer an integrated system — applications to disk — where all the pieces fit and work together so customers do not have to do it themselves."

■ No assembly required. Minimal customization possible. Self-upgrading, self-managing, stick-it-in-a-closet simple. Now *that's* an appliance.

Most analysts assume that means Oracle will be able to provide all the pieces customers need — just like IBM. A few think it means Oracle is planning to offer an easy-to-manage midrange system that includes a database and applications, modeled on what used to be called the AS/400 — again, just like IBM.

But what if it *really* means that Oracle wants to build an appliance? Not a database or storage appliance, like the machines Oracle and HP announced last fall, but a true application appliance, built from Sparc, Solaris, Oracle and application software, fully integrated, tuned and ready to use.

Say, for example, PeopleSoft-in-a-box.

No assembly required. Minimal customization possible. Self-upgrading, self-managing, stick-it-in-a-closet simple.

Now *that's* an appliance — not one for corporate IT shops, but one that would open up an entirely new market for Oracle: smaller customers who would gladly pay extra to avoid having to master the weirdness of enterprise applications.

That would let Oracle grow a hardware business with the margins of a software business.

Better still, it wouldn't cannibalize Oracle's current high-end software customers. It wouldn't compete directly with HP. And it could give Sparc and Solaris the volume to justify Oracle keeping Sun's traditional servers and other data center hardware alive.

Can Oracle do it? *Will* Oracle do it? I don't know, but Larry Ellison does love appliances. He's been trying for years to make appliances with partners — but without much success. Now Oracle will own all the pieces, including the hardware. This time, it just might work.

If you're a corporate IT shop with Sun hardware, pray that it does. ■

Frank Hayes *is Computerworld's senior news columnist. Contact him at frank_hayes@computerworld.com.*

VISIBILITY: 100%
EFFICIENCY: UP 43%
PAYBACK: 9 MONTHS
VALUE: 100% CLEAR

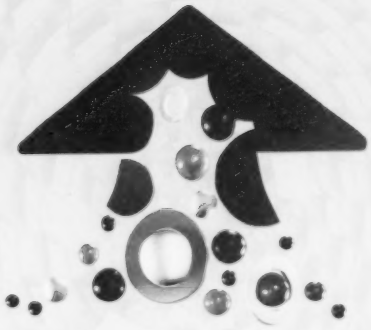
CA Spectrum® solutions help you pinpoint and solve information flow problems across the IT infrastructure — networks, physical and virtual systems, databases and applications — before they impact your end users. Eliminate costly, labor-intensive oversight and deliver seamless service with payback in under a year. That's the power of lean.

Read the IDC white paper on CA software and ROI at ca.com/spectrum.

ca Software

Copyright © 2009 CA. All rights reserved.

Deal with the virtual — and reality.



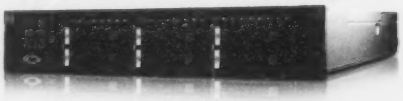
ALTERNATIVE THINKING ABOUT CONTROL AND CONSOLIDATION:

Manage and optimize your virtual and physical servers in the same way with HP Insight Dynamics — VSE.

When it comes to IT, your universe is always expanding. Needs increase, resources are stretched and options can be limited. But now, you can rethink how you control and optimize your physical and virtual servers by integrating them with one powerful software solution, Insight Dynamics — VSE. Now you can increase flexibility, improve cost and energy efficiency, and simplify daily operations.

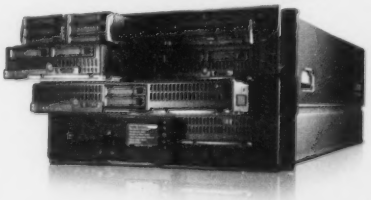
Supporting this technology is HP's commitment to service and dependability — a point of difference that led IDC to name HP the #1 vendor for virtualization.*

Technology for better business outcomes.



HP ProLiant DL Servers

- Quad-Core AMD Opteron™ Processor, with AMD Virtualization™ technology
- Ideal for general-purpose solutions and high-performance computing
- Affordable, modular rack systems to give your IT department the flexibility to expand with your business



HP BladeSystem c-Class

- Quad-Core AMD Opteron™ Processor, with AMD Virtualization™ technology
- Infrastructure-in-a-box saves you time, power and money by reducing repetitive parts and redundant operations
- Add, replace and recover resources on the fly without rewiring

AMD Opteron 64

To learn more, call 1-888-367-2308 or visit hp.com/servers/virtual9

AMD, the AMD arrow logo, AMD Opteron and combinations thereof, are trademarks of Advanced Micro Devices, Inc.
© 2009 Hewlett-Packard Development Company, L.P. The information contained herein is subject to change without notice.
*Source: IDC Quarterly Server Virtualization Tracker, October 2008.